MULTIPLICATIVE STRING ORIENTATIONS OF P-LOCAL AND P-COMPLETE REAL K-THEORY

Dissertation zur Erlangung des Doktorgrades
der Naturwissenschaften (Dr. rer. nat.)
der Fakultät für Mathematik
der Universität Regensburg

vorgelegt von
Christian Nerf
aus Roding

Regensburg, im März 2014

Promotionsgesuch eingereicht am: 31. März 2014

Diese Arbeit wurde angeleitet von: Prof. Dr. Niko Naumann

Prüfungsausschuss:

Vorsitzender:	Prof. Dr. Helmut Abels
Erst-Gutachter:	Prof. Dr. Niko Naumann
Zweit-Gutachter:	Prof. Dr. Ulrich Bunke
weiterer Prüfer:	Prof. Dr. Bernd Ammann

Contents

1 Introduction

Motivation and statement of results

It is assumed that the reader is familiar with stable homotopy theory and the theory of Bousfield localizations. We start with the following

Problem 1. *Is the set of string-orientations*

$$\pi_0 E_\infty(MString, KO)$$

empty and if not, how can we describe it?

In the article [AHR] Ando, Hopkins and Rezk gave a method to solve this problem. They showed that $\pi_0 E_\infty(MString, KO)$ is non-empty, but with their description it is hard to decide if this set has more than one element. This leads to the following

Problem 2. *Is there more than one element in $\pi_0 E_\infty(MString, KO)$?*

The goal of this work is to describe three results which are potentially helpful to attack Problem 2. These results are motivated by the strategy Ando-Hopkins-Rezk used to describe $\pi_0 E_\infty(MString, KO)$. They used the Sullivan arithmetic square

$$\begin{tikzcd} KO \arrow[r] \arrow[d] & \prod_p KO_p^\wedge \arrow[d] \\ KO \otimes \mathbb{Q} \arrow[r] & \prod_p (KO_p^\wedge \otimes \mathbb{Q}) \end{tikzcd}$$

to split Problem 1 up into the easier parts of determining

$$\pi_0 E_\infty(MString, KO \otimes \mathbb{Q}), \quad \pi_0 E_\infty(MString, KO_p^\wedge \otimes \mathbb{Q}) \text{ and } \pi_0 E_\infty(MString, KO_p^\wedge)$$

for all primes p. It is rather easy to show that

$$\pi_0 E_\infty(MString, KO \otimes \mathbb{Q}) = \prod_{\substack{k \geq 4 \\ k \text{ even}}} \mathbb{Q} \quad \text{and} \quad \pi_0 E_\infty(MString, KO_p^\wedge \otimes \mathbb{Q}) = \prod_{\substack{k \geq 4 \\ k \text{ even}}} \mathbb{Q}_p.$$

The hard part is to describe

$$\pi_0 E_\infty(MString, KO_p^\wedge)$$

for every prime p. For this Ando-Hopkins-Rezk used p-adic measure theory. For a compact and totally disconnected topological space X (in this work mainly $\mathbb{Z}_p$, $\mathbb{Z}_p^\times$ and $\mathbb{Z}_p^\times/\{\pm 1\}$) a p-adic measure μ is a continuous $\mathbb{Z}_p$-module homomorphism

$$\mu : \mathrm{cts}(X, \mathbb{Z}_p) \to \mathbb{Z}_p$$

and we use the notation

$$\int_X f d\mu := \mu(f)$$

where $f : X \to \mathbb{Z}_p$ is a continuous function. The set of such measures is denoted by $M(X, \mathbb{Z}_p)$.

In [AHS], for every $c \in \mathbb{Z}_p^\times$ which projects to a topological generator of

$$G := \mathbb{Z}_p^\times/\{\pm 1\}$$

the authors constructed an injective map

$$\mathrm{ahr}_c : \pi_0 E_\infty(MString, KO_p^\wedge) \to M(G, \mathbb{Z}_p).$$

Then they proved

Theorem ([AHR, Proposition 7.10]). *The image (denoted $\mathbf{AHR}_c$) of the map*

$$\pi_0 E_\infty(MString, KO_p^\wedge) \xrightarrow{\mathrm{ahr}_c} M(G, \mathbb{Z}_p)$$

is given by the set of measures μ which satisfy the following properties:

i) There exists an unique sequence

$$(b_k) \in \prod_{\substack{k\geq 4\\ k \text{ even}}} \mathbb{Q}_p$$

such that

$$\int_G \bar{x}^k d\mu(\bar{x}) = (1-c^k)(1-p^{k-1})b_k$$

for all even $k \geq 4$.

ii) For all even $k \geq 4$ we have

$$b_k \equiv -\frac{B_k}{2k} \mod \mathbb{Z}_p$$

where B_k is the k-th Bernoulli number.

Then Ando-Hopkins-Rezk showed that there exists at least one measure (called the Bernoulli measure) which satisfies this conditions. But with this description it is not easy to decide if the Bernoulli measure is the only element in $\mathbf{AHR}_c$. With Problem 2 in mind it is interesting to find a description of $\pi_0 E_\infty(MString, KO_p^\wedge)$ which shows how many elements are contained in this set. This question will be answered in

Theorem A. *Let $c \in \mathbb{Z}_p^\times$ be an element which projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$. Let*

$$\tilde{q} := \begin{cases} p-1 & \text{if } p \text{ odd} \\ 2 & \text{if } p = 2 \end{cases} \quad \text{and} \quad q := \begin{cases} p & \text{if } p \text{ odd} \\ 4 & \text{if } p = 2 \end{cases}.$$

We take an arbitrary element

$$(F_r)_{r\in I} \in \left(T\mathbb{Z}_p[\![T]\!] \oplus \bigoplus_{I-\{0\}} \mathbb{Z}_p[\![T]\!] \right)$$

where I is the set of even elements in $\mathbb{Z}/\tilde{q}$. Then there exists an unique measure $\mu \in \mathbf{AHR}_c$ such that

$$\int_G \bar{x}^k d\mu(\bar{x}) = F_k\big((1+q)^k - 1\big) - (1-c^k)(1-p^{k-1})\frac{B_k}{2k}.$$

Moreover the map

$$\left(T\mathbb{Z}_p[\![T]\!] \oplus \bigoplus_{I-\{0\}} \mathbb{Z}_p[\![T]\!]\right) \xrightarrow{\sim} \mathbf{AHR}_c \cong \pi_0 E_\infty(MString, KO_p^\wedge)$$

$$(F_r)_{r\in I} \mapsto \mu$$

is a bijection.

In particular $\pi_0 E_\infty(MString, KO_p^\wedge)$ contains uncountable many elements. Maybe this is not really surprising because there exists a natural occurring G-action on the set $\pi_0 E_\infty(MString, KO_p^\wedge)$ (which is given by the Adams operation $\psi_g : KO_p^\wedge \to KO_p^\wedge$ at $g \in G$) and there exists at least one element $\alpha_p \in \pi_0 E_\infty(MString, KO_p^\wedge)$. It is not so hard to see that there are uncountable many elements in the orbit $G\alpha_p$ of the G-action. Therefore it is interesting how many elements are contained in

$$G \setminus \pi_0 E_\infty(MString, KO_p^\wedge).$$

This question will be answered in

Theorem B. *The quotient set*

$$G \setminus \pi_0 E_\infty(MString, KO_p^\wedge)$$

contains uncountable many elements.

Another idea to attack Problem 2 is to give a description of

$$\pi_0 E_\infty(MString, KO_{(p)}) \subseteq \pi_0 E_\infty(MString, KO_p^\wedge)$$

and then use arithmetic squares. Unfortunately $\pi_0 E_\infty(MString, KO_{(p)})$ is much harder to determine. But we can show that there exists an uncountable infinite subset of $\pi_0 E_\infty(MString, KO_{(p)})$. With $\mathbf{AHR}_c^{loc}$ we denote the image of the map

$$\pi_0 E_\infty(MString, KO_{(p)}) \xrightarrow{\subseteq} \pi_0 E_\infty(MString, KO_p^\wedge) \xrightarrow{\mathrm{ahr}_c} \mathbf{AHR}_c.$$

With $c_0(\mathbb{Z}_p)$ we denote the set of zero sequences over $\mathbb{Z}_p$. Then we have

Theorem C. *Let $c \in \mathbb{Z}_{(p)} \subseteq \mathbb{Z}_p^\times$ be an element which projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$. With $\mathbf{Y} \subseteq c_0(\mathbb{Z}_p)$ we denote the subset of elements $(b_n)_{n\geq 0} \in c_0(\mathbb{Z}_p)$ which fulfil the following properties:*

i) For all $n \geq 0$ we have $b_n \in \mathbb{Z}_{(p)}$.

ii) For all $n \geq 0$ we have

$$\frac{b_n}{n!p^n} \in \mathbb{Z}_p.$$

Let

$$\mathbf{Y}_0 := \{(b_n)_{n\geq 0} \in \mathbf{Y} \mid b_0 = 0\}.$$

and let $\hat{p}_k := p^{-1}\big((1+q)^k - 1\big)$. We take an arbitrary element

$$\Big((b_{r,n})_{n\geq 0}\Big)_{r\in I} \in \left(\mathbf{Y}_0 \oplus \bigoplus_{r\in I-\{0\}} \mathbf{Y}\right)$$

where I is the set of even elements in $\mathbb{Z}/\tilde{q}$. Then there exists an unique measure $\mu \in \mathbf{AHR}_c^{loc}$ such that

$$\int_G \bar{x}^k d\mu(\bar{x}) = \left(\sum_{n=0}^{\hat{p}_k} b_{k,n} \binom{\hat{p}_k}{n} \right) - (1-c^k)(1-p^{k-1}) \frac{B_k}{2k}.$$

Moreover the map

$$\left(\mathbf{Y}_0 \oplus \bigoplus_{r \in I - \{0\}} \mathbf{Y} \right) \hookrightarrow \mathbf{AHR}_c^{loc} \cong \pi_0 E_\infty(MString, KO_{(p)})$$

$$\Big((b_{r,n})_{n \geq 0} \Big)_{r \in I} \mapsto \mu$$

is an injection.

Strategy and organisation

This work is organized in Sections, Subsections and Paragraphs. The idea for reaching the goal of describing $\pi_0 E_\infty(MString, KO_p^\wedge)$ is to reduce this problem to the following

Problem 3. *Let $c \in \mathbb{Z}_p^\times$ be an element which projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$. What is*

$$\Gamma^{-1}(\mathbf{ConA}_c)$$

where

i)

$$\Gamma : \bigoplus_{\substack{r \in \mathbb{Z}/\tilde{q} \\ r \text{ even}}} \mathbb{Z}_p[\![T]\!] \to \prod_{\substack{k \geq 4 \\ k \text{ even}}} \mathbb{Q}_p$$

is defined by

$$(F_r) \mapsto \Big(F_k\big((1+q)^k - 1\big) \Big).$$

ii) $\mathbf{ConA}_c$ is the set of elements

$$(z_k) \in \operatorname{Im}(\Gamma)$$

which satisfy

$$z_k \in (1-c^k)\mathbb{Z}_p$$

for all even $k \geq 4$ which fulfil the property that $1 - c^k \in p\mathbb{Z}_p$.

In Section 2 we solve this problem. In the first subsection 2.1 we collect some facts about p-adic analysis and topological generators which are needed later. In Subsection 2.2 we show that

$$\Gamma^{-1}(\mathbf{ConA}_c) = \left\{ (F_r) \in \bigoplus_{\substack{r \in \mathbb{Z}/\tilde{q} \\ r \text{ even}}} \mathbb{Z}_p[\![T]\!] \;\middle|\; F_0(0) = 0 \right\}.$$

The goal of the Section 3 to construct an isomorphism

$$\Phi_1 : M(G, \mathbb{Z}_p) \xrightarrow{\sim} \bigoplus_{\substack{r \in \mathbb{Z}/\tilde{q} \\ r \text{ even}}} \mathbb{Z}_p[\![T]\!]$$

such that the diagram

$$\begin{array}{ccc} \mu & \quad & \begin{tikzcd} M(G,\mathbb{Z}_p) \arrow[r, "\sim"] \arrow[d] & \bigoplus\limits_{\substack{r\in\mathbb{Z}/\tilde{q} \\ r \text{ even}}} \mathbb{Z}_p[\![T]\!] \arrow[dl, "\Gamma"] \\ \prod\limits_{\substack{k\geq 4 \\ k \text{ even}}} \mathbb{Q}_p & \end{tikzcd} \\ \downarrow & & \\ \left(\int\limits_G \bar{x}^k d\mu(\bar{x})\right) & & \end{array}$$

commutes. This construction is a special case of a construction which is made in [W]. In Subsection 3.1 and 3.2 we recall some facts about p-adic continuous functions and p-adic measure theory. In Subsection 3.3 and 3.4 we construct the isomorphism Φ_1.

Remember that Ando-Hopkins-Rezk proved the existence of an element

$$\alpha_p \in \pi_0 E_\infty(MString, KO_p^\wedge).$$

With $(F_r^{Ber}) \in \bigoplus_{\substack{r\in\mathbb{Z}/\tilde{q} \\ r \text{ even}}} \mathbb{Z}_p[\![T]\!]$ we denote the image of α_p under the map

$$\Phi : \pi_0 E_\infty(MString, KO_p^\wedge) \xrightarrow{\text{ahr}_c} M(G,\mathbb{Z}_p) \xrightarrow{\sim} \bigoplus_{\substack{r\in\mathbb{Z}/\tilde{q} \\ r \text{ even}}} \mathbb{Z}_p[\![T]\!].$$

In the first paragraph of Subsection 3.5 we prove that the image of this map is given by the set

$$\mathrm{im}(\Phi) = (F_r^{Ber}) + \Gamma^{-1}(\mathbf{ConA}_c).$$

Then we show that this imply Theorem A. In the second and third paragraph of Subsection 3.5 we prove Theorem B and Theorem C. The proofs of this theorems uses mainly the following observations:

O1) The set $M(G,\mathbb{Z}_p)$ carries the structure of a G-set and the injective map

$$\pi_0 E_\infty(MString, KO_p^\wedge) \xrightarrow{\text{ahr}_c} M(G,\mathbb{Z}_p)$$

is G-equivariant.

O2) The bijection

$$M(G,\mathbb{Z}_p) \xrightarrow{\sim} \bigoplus_{\substack{r\in\mathbb{Z}/\tilde{q} \\ r \text{ even}}} \mathbb{Z}_p[\![T]\!]$$

endows the right hand side with the structure of a G-set. The quotient

$$G \setminus \bigoplus_{\substack{r\in\mathbb{Z}/\tilde{q} \\ r \text{ even}}} \mathbb{Z}_p[\![T]\!]$$

contains uncountable many elements.

O3) The image of the map

$$\pi_0 E_\infty(MString, KO_{(p)}) \xrightarrow{\subseteq} \pi_0 E_\infty(MString, KO_p^\wedge) \xrightarrow{\Phi} \bigoplus_{\substack{r\in\mathbb{Z}/\tilde{q} \\ r \text{ even}}} \mathbb{Z}_p[\![T]\!].$$

is given by the set

$$\Gamma^{-1}(\mathbf{ConB}_c)$$

where

$$\mathbf{ConB}_c := \Big((F_r^{Ber}) + \Gamma^{-1}(\mathbf{ConA}_c)\Big) \cap \prod_{\substack{k\geq 4 \\ k \text{ even}}} \mathbb{Z}_{(p)}.$$

Observation 1 is proven in Section 4. For this proof we repeat the construction of the map ahr_c made in [AHR] and show that every part is G-equivariant.

Observation 2 is proven during the construction of the map

$$M(G, \mathbb{Z}_p) \xrightarrow{\sim} \bigoplus_{\substack{r\in\mathbb{Z}/\tilde{q} \\ r \text{ even}}} \mathbb{Z}_p[\![T]\!]$$

made in the Subsections 3.3 and 3.4. To prove Theorem B in Subsection 3.5 we have only to show that the quotient

$$G \setminus \bigoplus_{\substack{r\in\mathbb{Z}/\tilde{q} \\ r \text{ even}}} \mathbb{Z}_p[\![T]\!]$$

contains uncountable many elements.

The proof of Observation 3 uses arithmetic squares like in [AHR] and is found in Subsection 4.3. To deduce Theorem C out of Observation 3 we construct an isomorphism

$$\bigoplus_{\substack{r\in\mathbb{Z}/\tilde{q} \\ r \text{ even}}} \mathbb{Z}_p[\![T]\!] \xrightarrow{\sim} \bigoplus_{\substack{r\in\mathbb{Z}/\tilde{q} \\ r \text{ even}}} \mathbf{X}$$

where $\mathbf{X}$ is defined to be the set of zero sequences $(b_n)_{n\geq 0} \in c_0(\mathbb{Z}_p)$ such that $\frac{b_n}{n!p^n} \in \mathbb{Z}_p$ for all $n \geq 0$. This is a slightly modified version of a Theorem found in [Laz]. During the constructions made in Section 3 we show that the diagram

$$\begin{tikzcd}
M(G,\mathbb{Z}_p) \arrow[r, "\sim"] & \bigoplus_{\substack{r\in\mathbb{Z}/\tilde{q} \\ r \text{ even}}} \mathbb{Z}_p[\![T]\!] \arrow[r, "\sim"] \arrow[d, "\Gamma"] & \bigoplus_{\substack{r\in\mathbb{Z}/\tilde{q} \\ r \text{ even}}} \mathbf{X} \arrow[dl, "\tilde{\Gamma}"] \\
& \prod_{\substack{k\geq 4 \\ k \text{ even}}} \mathbb{Q}_p &
\end{tikzcd}$$

commutes, where $\tilde{\Gamma}$ maps an element $\Big((b_{r,n})_{n\geq 0}\Big)_r$ to the element

$$\left(\sum_{n=0}^{\hat{p}_k} b_{k,n} \binom{\hat{p}_k}{n}\right)_{\substack{k\geq 4 \\ k \text{ even}}}$$

with $\hat{p}_k := p^{-1}\big((1+q)^k - 1\big)$. The problem of determining

$$\hat{\Gamma}^{-1}(\mathbf{ConB}_c)$$

is easier then determining

$$\Gamma^{-1}(\mathbf{ConB}_c)$$

but still open. But it is possible to describe an uncountable large subset of $\hat{\Gamma}^{-1}(\mathbf{ConB}_c)$ which is described in Theorem C.

The hope was, that Theorem A, Theorem B and Theorem C can help to solve Problem 2. This problem is still unsolved.

Acknowledge

I would like to express my gratitude to several people. First of all, I want to thank Prof. Dr. Niko Naumann. He was my advisor and supported the whole work from the beginning till its completion. Then I want to thank Prof. Dr. David Gepner, Prof. Dr. Ulrich Bunke and Dr. Thomas Nikolaus for their organisation of several very helpful seminars and lectures, and for always being ready to answer questions. Finally I want to thank Peter Arndt, Martin Ruderer and Micheal Völkl and the other members of the Graduiertenkolleg "Curvature, Cycles and Cohomology" for several interesting and helpful discussions about mathematics and many other subjects.

Notation

- Let R be a ring and $n \geq 0$. The notation $F(T) = \mathcal{O}(T^n) \in R[\![T]\!]$ means that there exists a polynomial $P(T) \in T^n R[\![T]\!]$ such that $F(T) = P(T)$.
- If X, Y are topological spaces, we denote the set of continuous function between X and Y with $\mathrm{cts}(X, Y)$.
- The Symbol Δ has two meanings. In some subsections it is the difference function
$$\Delta : \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p) \to (\mathbb{Z}_p, \mathbb{Z}_p)$$
$$f(x) \mapsto f(x+1) - f(x),$$
in some others subsections it stands for the set $(\mathbb{Z}/q\mathbb{Z})^\times/\{\pm 1\}$. The two meanings never appear in the same subsection. Since out of the context it is clear what meaning is meant, I am convinced that there is no danger that there will be a confusion.
- For a given prime p we use always the following notations:
$$q := \begin{cases} p & \text{if } p \text{ odd} \\ 4 & \text{if } p = 2 \end{cases}$$
and
$$\tilde{q} := \begin{cases} p-1 & \text{if } p \text{ odd} \\ 2 & \text{if } p = 2 \end{cases} .$$
- For an even positive integer $\tilde{q}$ and a ring R we write
$$\bigoplus_{r \in \mathbb{Z}/\tilde{q}}^{*} R \quad \text{for} \quad \bigoplus_{\substack{r \in \mathbb{Z}/\tilde{q} \\ r \text{ even}}} R$$
and
$$(z_r)^*_{r \in \mathbb{Z}/\tilde{q}} \quad \text{for} \quad (z_r)_{\substack{r \in \mathbb{Z}/\tilde{q} \\ r \text{ even}}} .$$
Further we write
$$\prod_{k \geq 4}^{*} R \quad \text{for} \quad \prod_{\substack{k \geq 4 \\ k \text{ even}}} R$$
and
$$(z_k)^*_{k \geq 4} \quad \text{for} \quad (z_k)_{\substack{k \geq 4 \\ k \text{ even}}} .$$

2 p-adic analysis

For the rest of this section we fix a prime p.

2.1 Foundations of p-adic analysis

This section reviews the basics of p-adic analysis and topologically cyclic groups and we give some preparation for the later parts of this work. The theory in this subsection can be found in many books, e.g. [N], [W] or [Ko].

The p-adic numbers and their topology

The p-adic valuation is a function
$$v_p : \mathbb{Q}^\times \to \mathbb{R}$$
mapping a rational $x = \frac{a}{b} \in \mathbb{Q}$ to the unique integer m such that
$$x = p^m \frac{a'}{b'} \text{ with } (a', p) = (b', p) = 1.$$
The p-adic norm is given by
$$|x|_p = p^{-v(x)}.$$
Formally we set $v_p(0) = \infty$ and $|0|_p = 0$. This norm induces a non-complete metric on $\mathbb{Q}$, i.e. not every Cauchy sequence in $(\mathbb{Q}, |.|_p)$ is convergent. The field of p-adic numbers $\mathbb{Q}_p$ is defined to be the completion of $(\mathbb{Q}, |.|_p)$. The p-adic valuation and p-adic norm extend in a canonical way to $\mathbb{Q}_p$. The p-adic integers are defined to be the set
$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p | v_p(x) \geq 0\}.$$
The p-adic valuation gives $\mathbb{Z}_p$ the structure of a discrete valuation ring with residue field $\mathbb{F}_p$. Thus
$$\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p | v_p(x) = 0\}$$
and the unique maximal in $\mathbb{Z}_p$ is given by
$$p\mathbb{Z}_p = \{x \in \mathbb{Q}_p | v_p(x) > 0\}.$$
Every p-adic number $x \in \mathbb{Q}_p - \{0\}$ has a unique p-adic expansion, i.e. there exists a unique formal infinite sum
$$x = \sum_{i=-\infty}^{\infty} a_i p^i \quad a_i \in \{0, 1, \ldots, p-1\}$$
such that there exists $m \in \mathbb{Z}$ such that $a_i = 0$ for $i < m$ and $a_m \neq 0$. It turns out that $m = v_p(x)$. There exists a ring isomorphism
$$\mathbb{Z}_p \to \lim(\cdots \to \mathbb{Z}/p^3\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}) = \lim \mathbb{Z}/p^n\mathbb{Z}$$
$$\sum_{i=0}^{\infty} a_i p^i \mapsto \left(\sum_{i=0}^{n-1} a_i p^i \right)_{n \geq 1}$$
and it turns out that there is an isomorphism
$$\mathbb{Z}_p^\times \to \lim(\mathbb{Z}/p^n\mathbb{Z})^\times.$$

Note that $|(\mathbb{Z}/p^n\mathbb{Z})^\times| = (p-1)p^{n-1}$. For a p-adic unit $c \in \mathbb{Z}_p^\times$ we have

$$c^{(p-1)p^{n-1}} \equiv 1 \mod p^n$$

for $n \geq 1$.

We now collect some facts about the topology of $\mathbb{Q}_p$ found for example in [W], [Ko] or [N].

i) Since $\mathbb{Z}_p$ is a limit of finite sets it is compact.

ii) The set $\mathbb{Z}_p$ is totally disconnected, i.e. the only connected components in $\mathbb{Z}_p$ are the one-point sets.

iii) The subset $\mathbb{N}_0 \subseteq \mathbb{Z}_p$ is dense.

iv) The sets
$$a + p^n\mathbb{Z}_p, \qquad a \in \mathbb{Q}_p, n \in \mathbb{Z}$$
form a basis of the p-adic topology. Sets of this form are called intervals.

v) An open subset of $\mathbb{Q}_p$ is compact if and only if it is a finite union of intervals.

vi) For all $x, y \in \mathbb{Z}_p$ we have that
$$v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$$
with equality if $v_p(x) \neq v_p(y)$.

The p-adic logarithm

A important difference to real analysis is that over $\mathbb{Q}_p$ a series $\sum \alpha_n$ converges if and only if (α_n) is a null sequence. This can be used to calculate the convergence radii of the logarithm and exponential series

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

and

$$\log_p(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}.$$

It turns out[1] that the convergence radius for $\exp(x)$ is $p^{-1/(p-1)}$ and the convergence radius for $\log_p(1+x)$ is 1. For fitting $x, y \in \mathbb{Z}_p$ and $n \in \mathbb{Z}$ we have the usual properties:

$$\exp(x+y) = \exp(x)\exp(y) \quad \text{and} \quad \log_p(xy) = \log_p x + \log_p y$$

and

$$n \log_p x = \log_p x^n.$$

In analogy to real analysis we want to define

$$a^x = \exp(x \log_p(a)), \quad x \in \mathbb{Z}_p$$

and have to decide for which $a \in \mathbb{Z}_p$ this makes sense. The answer we give in the corollary to the following

[1] See for example [W, page 49-50]

Proposition 4 ([W], Lemma 5.5, Proposition 5.7)**.** *If* $|x|_p < p^{-1/(p-1)}$ *then*

$$\log_p \exp(x) = x, \quad \exp \log_p(1+x) = 1+x$$

and

$$|\log_p(1+x)|_p = |x|_p.$$

We use the notation

$$q = \begin{cases} p, & \text{if } p \neq 2 \\ 4, & \text{if } p = 2. \end{cases}$$

Note that

$$|x|_p < p^{-1/(p-1)} \Leftrightarrow v_p(x) > \frac{1}{p-1} \Leftrightarrow v_p(x) \geq \begin{cases} 1, & \text{if } p \neq 2 \\ 2, & \text{if } p = 2 \end{cases} \Leftrightarrow x \in q\mathbb{Z}_p.$$

In other words, Proposition 4 states that we have an isomorphism of topological groups

$$\exp : q\mathbb{Z}_p \xrightarrow{\sim} 1 + q\mathbb{Z}_p$$

with inverse given by

$$\log_p : 1 + q\mathbb{Z}_p \xrightarrow{\sim} q\mathbb{Z}_p.$$

Corollary 5. *Let* $a \in 1 + q\mathbb{Z}_p$.

i) The assignment

$$x \mapsto a^x := \exp(x \log_p(a))$$

gives a well defined continuous group homomorphism

$$a^\bullet : \mathbb{Z}_p \to 1 + q\mathbb{Z}_p.$$

For $n \in \mathbb{Z}$ *the value* a^n *agrees with the usual definition.*

ii) The assignment

$$x \mapsto \frac{\log_p x}{\log_p 1+q}$$

gives a well defined continuous group homomorphism

$$l_p : 1 + q\mathbb{Z}_p \to \mathbb{Z}_p.$$

The maps $(1+q)^\bullet$ *and* l_p *are inverse group isomorphisms.*

Proof. For i): We have a chain of implications

$$a \in 1 + q\mathbb{Z}_p \Rightarrow \log a \in q\mathbb{Z}_p \Rightarrow x \log a \in q\mathbb{Z}_p \Rightarrow a^x = \exp(x \log_p(a)) \in 1 + q\mathbb{Z}_p.$$

Thus $a^\bullet$ is well defined. Since exp is continuous we know that $a^\bullet$ is continuous. Further, $a^\bullet$ is obviously a group homomorphism. Since a^n in the usual definition is an element of $1 + q\mathbb{Z}_p$, Proposition 4 states that the new definition of a^n agrees with the usual definition.

For ii): Proposition 4 states that $|\log_p(1-q)|_p = |q|_p$ and since $|\log_p x|_p = |qy|_p$ with $y \in \mathbb{Z}_q$ we have

$$|l_p x|_p = \left| \frac{\log_p x}{\log_p 1+q} \right|_p = \frac{|q|_p |y|_p}{|q|_p} = |y|_p \leq 1,$$

i.e. l_p is well defined. Because $\log_p$ is continuous we know that l_p is continuous. Further, l_p is obviously a group homomorphism. It remains to show that $(1+q)^\bullet$ and l_p are inverse group isomorphisms. We have

$$(1+q)^{l_p x} = \exp\left(\frac{\log_p x}{\log_p 1+q}\log_p 1+q\right) = x$$

and

$$l_p((1+q)^x) = \frac{\log_p \exp(x\log_p(1+q))}{\log_p 1+q} = x.$$

□

Hensel's lemma

In the following we need the fact that $\mathbb{Z}_p^\times$ contains the $(p-1)$st roots of unity. This is an easy consequence of

Theorem 6 (Hensel's Lemma). *Let $F(T) \in \mathbb{Z}_p[T]$ and $F'(T)$ the formal derivative of F. Let a be a p-adic integer such that*

$$F(a) \equiv 0 \mod p \quad \text{and} \quad F'(a) \not\equiv 0 \mod p.$$

Then there exists a p-adic integer b such that

$$F(b) = 0 \quad \text{and} \quad a \equiv b \mod p.$$

A proof for the Theorem can be found for example in [Ko] (Chapter I, Theorem 3).

Example 7. The polynomial

$$T^{p-1} - 1 \in \mathbb{Z}_p[T]$$

decomposes into linear factors modulo $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$. Thus Hensel's lemma states that $\mathbb{Z}_p^\times$ contains the $(p-1)$st roots of unity μ_{p-1}. Obviously $\mu_2 \subseteq \mathbb{Z}_2^\times$. Let φ be Euler's phi function, i.e.

$$\varphi(q) = \begin{cases} p-1, & \text{if } p \neq 2 \\ 2, & \text{if } p = 2. \end{cases}$$

If we restrict the canonical homomorphism

$$\mathbb{Z}_p^\times \to (\mathbb{Z}/q\mathbb{Z})^\times$$

to $\mu_{\varphi(q)} \subseteq \mathbb{Z}_p^\times$, Hensel's lemma implies that we get a canonical isomorphism

$$\sigma : \mu_{\varphi(q)} \to (\mathbb{Z}/q\mathbb{Z})^\times$$

with

$$\zeta \mapsto \zeta \mod q.$$

This means that the exact sequence

$$0 \to 1 + q\mathbb{Z}_p \to \mathbb{Z}_p^\times \to (\mathbb{Z}/q\mathbb{Z})^\times \to 0$$

is split which implies the following

Corollary 8. *There is a canonical splitting*

$$(\omega(.), \langle.\rangle) : \mathbb{Z}_p^\times \xrightarrow{\sim} \mu_{\varphi(q)} \times (1+q\mathbb{Z}_p) \xrightarrow{\sim} (\mathbb{Z}/q\mathbb{Z})^\times \times (1+q\mathbb{Z}_p).$$

We define the Teichmüller character to be the homomorphism

$$\omega : \mathbb{Z}_p^\times \xrightarrow{\sim} \mu_{\varphi(q)} \times (1+q\mathbb{Z}_p) \xrightarrow{pr_1} \mu_{\varphi(q)} \subseteq \mathbb{Z}_p^\times,$$

i.e. $\omega(x)$ is the unique $\varphi(q)$st root of unity such that $x \equiv \omega(x) \mod q$. Further, we define

$$\langle.\rangle : \mathbb{Z}_p^\times \xrightarrow{\sim} \mu_{\varphi(q)} \times (1+q\mathbb{Z}_p) \xrightarrow{pr_2} 1+q\mathbb{Z}_p,$$

i.e. $x = \omega(x)\langle x\rangle$.

Lemma 9. *The homomorphisms $\omega : \mathbb{Z}_p^\times \to \mu_{\varphi(q)}$ and $\langle.\rangle : \mathbb{Z}_p^\times \to 1+q\mathbb{Z}_p$ are continuous.*

Proof. Let $(a_n) \subseteq \mathbb{Z}_p^\times$ be a sequence converging to $a \in \mathbb{Z}_p^\times$, i.e.

$$\omega(a_n)\langle a_n\rangle \to \omega(a)\langle a\rangle.$$

Let $a = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \dots$. Since $\alpha_0 + q\mathbb{Z}_p$ is an open neighbourhood of a we know that $a_n \in \alpha_0 + q\mathbb{Z}_p$ for infinite many n. Thus $\omega(a_n) = \omega(\alpha_0) = \omega(a)$ and

$$\omega(\alpha_0)\langle a_n\rangle \to \omega(\alpha_0)\langle a\rangle.$$

This implies $\langle a_n\rangle \to \langle a\rangle$ and $\omega(a_n) \to \omega(a)$. □

We use the notation $\Delta = (\mathbb{Z}/q\mathbb{Z})^\times/\{\pm 1\}$. Remember that Hensel's lemma gave us a canonical isomorphism

$$\sigma : \mu_{\varphi(q)} \to (\mathbb{Z}/q\mathbb{Z})^\times.$$

We denote the induced isomorphism

$$\sigma : \mu_{\varphi(q)}/\{\pm 1\} \to \Delta$$

also by σ.

Proposition 10. *The map*

$$(\sigma \circ \omega,\ l_p \circ \langle.\rangle) : \mathbb{Z}_p^\times \xrightarrow{\sim} (\mathbb{Z}/q\mathbb{Z})^\times \times (1+q\mathbb{Z}_p) \xrightarrow{\sim} (\mathbb{Z}/q\mathbb{Z})^\times \times \mathbb{Z}_p$$

$$x \mapsto ((\sigma\circ\omega)(x), \langle x\rangle) \mapsto \left((\sigma\circ\omega)(x), \frac{\log_p\langle x\rangle}{\log_p(1+q)}\right)$$

is an isomorphism of topological groups. The inverse isomorphism $(\mathbb{Z}/q\mathbb{Z})^\times \times \mathbb{Z}_p \xrightarrow{\sim} \mathbb{Z}_p^\times$ is given by $(g, x) \mapsto \sigma^{-1}(g)(1+q)^x$.

Proof. Corollary 8 together with Corollary 5. □

Note that ω and $\langle.\rangle$ induces continuous group homomorphisms

$$\omega : \mathbb{Z}_p^\times/\{\pm 1\} \xrightarrow{\sim} \mu_{\varphi(q)}/\{\pm 1\} \times (1+q\mathbb{Z}_p) \xrightarrow{pr_1} \mu_{\varphi(q)}/\{\pm 1\} \subseteq \mathbb{Z}_p^\times/\{\pm 1\},$$

and

$$\langle.\rangle : \mathbb{Z}_p^\times/\{\pm 1\} \xrightarrow{\sim} \mu_{\varphi(q)}/\{\pm 1\} \times (1+q\mathbb{Z}_p) \xrightarrow{pr_2} 1+q\mathbb{Z}_p.$$

Corollary 11. *The map*

$$(\sigma \circ \omega,\ l_p \circ \langle . \rangle) : \mathbb{Z}_p^\times/\{\pm 1\} \xrightarrow{\sim} \Delta \times (1 + q\mathbb{Z}_p) \xrightarrow{\sim} \Delta \times \mathbb{Z}_p$$

given by

$$x \mapsto ((\sigma \circ \omega)(x), \langle x \rangle) \mapsto \left((\sigma \circ \omega)(x), \frac{\log_p \langle x \rangle}{\log_p(1+q)} \right)$$

is an isomorphism of topological groups. The inverse isomorphism $\Delta \times \mathbb{Z}_p \xrightarrow{\sim} \mathbb{Z}_p^\times/\{\pm 1\}$ is given by $(g, x) \mapsto \sigma^{-1}(g)(1+q)^x$.

Topological generators

Let X be a topological group. An element $c \in X$ is called topological generator if $c^{\mathbb{Z}} \subseteq X$ is dense. From now on we call them only generators and say that X is topologically cyclic if there exists a generator $c \in X$. In the later parts of this work X will always be one of the groups $\mathbb{Z}_p$, $\mathbb{Z}_p^\times$, $\mathbb{Z}_p^\times/\{\pm 1\}$ or $1 + q\mathbb{Z}_p$. We start with an easy lemma.

Lemma 12. *Let $f : X \to Y$ be a surjective homomorphism of topological groups and $c \in X$ a generator. Then $f(c)$ is a generator of Y.*

Proof. The image of $c^{\mathbb{Z}}$ under f is dense in Y. Obviously $f(c)$ is a generator of $f(c^{\mathbb{Z}})$ □

Corollary 13. *Let X, Y be topological groups and $c = (c_1, c_2) \in X \times Y$ a generator. Then c_1 and c_2 are generators of X and Y.*

Proof. The maps $pr_1 : X \times Y \to X$ and $pr_2 : X \times Y \to Y$ are surjective. □

Example 14. i) Assume the topology on X is discrete. Then an element $c \in X$ is a generator of X if and only if c is a generator of X as a group.

ii) Since $\mathbb{Z} \subseteq \mathbb{Z}_p$ is dense it is obvious that $1 \in \mathbb{Z}_p$ is a generator. Assume an element $c \in \mathbb{Z}_p$ satisfies $v_p(c) = v_p(1)$. Then we have $c \in \mathbb{Z}_p^\times$ and multiplication with c gives obviously an isomorphism of topological groups

$$\mathbb{Z}_p \xrightarrow{\cdot c} \mathbb{Z}_p$$

with inverse given by

$$\mathbb{Z}_p \xrightarrow{\cdot c^{-1}} \mathbb{Z}_p.$$

We get that $c = c \cdot 1$ is a generator.

Assume $v_p(c) > v_p(1)$. Then $1 - cm \in 1 + p\mathbb{Z}_p$ for all $m \in \mathbb{Z}$. This implies $|1 - cm|_p = 1$ for all $m \in \mathbb{Z}$, i.e. $c\mathbb{Z}$ is not dense in $\mathbb{Z}_p$.

All together we have that an element $c \in \mathbb{Z}_p$ is a generator if and only if

$$v_p(c) = v_p(1) = 0.$$

iii) Note that there is a canonical isomorphism of topological groups

$$\lambda : q\mathbb{Z}_p \to \mathbb{Z}_p$$

where $\lambda(x)$ is the unique element $y \in \mathbb{Z}_p$ which satisfies $x = qy$. The inverse is given by multiplication with q.

Therefore an element $c \in q\mathbb{Z}_p$ is a generator if and only if $\lambda(c)$ is a generator of $\mathbb{Z}_p$. This is equivalent to $v_p(\lambda(c)) = 0$ and this is equivalent to

$$v_p(c) = v_p(q\lambda(c)) = v_p(q) + v_p(\lambda(c)) = v_p(q).$$

All together we have that an element $c \in q\mathbb{Z}_p$ is a generator if and only if

$$v_p(c) = v_p(q).$$

Lemma 15. *An element $c \in 1 + q\mathbb{Z}_p$ is generator if and only if*

$$v_p(c-1) = v_p(q) = \begin{cases} 1, & \text{if } p \neq 2 \\ 2, & \text{if } p = 2. \end{cases}$$

In particular $1 + q$ is a generator of $1 + q\mathbb{Z}_p$.

Proof. Remember that Proposition 4 gives us an isomorphism of topological groups

$$\log_p : 1 + q\mathbb{Z}_p \xrightarrow{\sim} q\mathbb{Z}_p$$

which satisfies $|\log_p(1+x)|_p = |x|_p$, i.e. $v_p(\log_p(1+x)) = v_p(x)$. Therefore an element $c \in 1+q\mathbb{Z}_p$ is a generator if and only if

$$\log_p(c) \in q\mathbb{Z}_p$$

is a generator. Part iii of Example 14 states that this is equivalent to

$$v_p(\log_p(c)) = v_p(q)$$

and this is equivalent to

$$v_p(c-1) = v_p(q).$$

□

The next goal is to give a description of the generators of the groups $\mathbb{Z}_p^\times$ and $\mathbb{Z}_p^\times/\{\pm 1\}$. Fist of all note that $\mathbb{Z}_2^\times$ is obviously not topologically cyclic, because $(\mathbb{Z}/8\mathbb{Z})^\times$ is not cyclic. We begin with a corollary to Lemma 15.

Corollary 16. *Let $l \in \mathbb{Z}_p^\times$. If c is a generator of $1 + q\mathbb{Z}_p$ then c^l is also a generator of $1 + q\mathbb{Z}_p$.*

Proof. The homomorphism of topological groups $q\mathbb{Z}_p \xrightarrow{\cdot l} q\mathbb{Z}_p$ is an isomorphism with inverse given by $q\mathbb{Z}_p \xrightarrow{\cdot l^{-1}} q\mathbb{Z}_p$. Further we have a commutative diagram

$$\begin{tikzcd} 1 + q\mathbb{Z}_p \arrow[r, "\log_p"] \arrow[d, "x \mapsto x^l"'] & q\mathbb{Z}_p \arrow[d, "x \mapsto lx"] \\ 1 + q\mathbb{Z}_p \arrow[r, "\log_p"'] & q\mathbb{Z}_p \end{tikzcd}$$

Since the horizontal maps and the right vertical map are isomorphisms, this is also true for the left vertical map. Therefore $1 + q\mathbb{Z}_p \xrightarrow{x \mapsto x^l} 1 + q\mathbb{Z}_p$ maps generators to generators. □

Proposition 17. *Let G be a finite group of order $< p$. Elements $g \in G$ and $c \in 1 + q\mathbb{Z}_p$ are generators if and only if (g, c) is a generator of $G \times (1 + q\mathbb{Z}_p)$.*

Proof. Assume $g \in G$ and $c \in 1 + q\mathbb{Z}_p$ are generators. We have

$$G \times (1 + q\mathbb{Z}_p) = \bigcup_{1 \leq l \leq |G|} \{g^l\} \times (1 + q\mathbb{Z}_p).$$

Corollary 16 states that c^l is a generator of $(1 + q\mathbb{Z}_p)$ for all $1 \leq l \leq |G| < p$. This imply that $(g, c)^{l\mathbb{Z}}$ is dense in $\{g^l\} \times (1 + q\mathbb{Z}_p)$ for all such l and this imply that

$$\bigcup_{1 \leq l \leq |G|} (g, c)^{l\mathbb{Z}} \subseteq (g, c)^{\mathbb{Z}}$$

is dense in $G \times (1 + q\mathbb{Z}_p)$.

Assume (g, c) is a generator. Corollary 13 states that g and c are generators. □

Proposition 18. *i) Except for $\mathbb{Z}_2^\times$ all of the groups $\mathbb{Z}_p^\times$ and $\mathbb{Z}_p^\times/\{\pm 1\}$ are topologically cyclic.*

ii) An element $c \in \mathbb{Z}_p^\times/\{\pm 1\}$ is a generator if and only if $\omega(c) \in \Delta$ and $\langle c \rangle \in (1 + q\mathbb{Z}_p)$ are generators.

iii) Let p be odd. An element $c \in \mathbb{Z}_p^\times$ is a generator if and only if $\omega(c) \in (\mathbb{Z}/p\mathbb{Z})^\times$ and $\langle c \rangle \in (1 + q\mathbb{Z}_p)$ are generators.

Proof. We have isomorphisms of topological groups

$$(\omega(.), \langle . \rangle) : \mathbb{Z}_p^\times \xrightarrow{\sim} (\mathbb{Z}/q\mathbb{Z})^\times \times (1 + q\mathbb{Z}_p)$$

and

$$(\omega(.), \langle . \rangle) : \mathbb{Z}_p^\times/\{\pm 1\} \xrightarrow{\sim} \Delta \times (1 + q\mathbb{Z}_p).$$

Note that $|\Delta| < p$ for all primes and $|(\mathbb{Z}/q\mathbb{Z})^\times| < p$ for all odd primes.

An element $c \in \mathbb{Z}_p^\times/\{\pm 1\}$ is a generator if and only if $(\omega(c), \langle c \rangle)$ is a generator of $\Delta \times (1+q\mathbb{Z}_p)$. Proposition 17 imply that is equivalent to the condition that $\omega(c) \in \Delta$ and $\langle c \rangle \in (1 + q\mathbb{Z}_p)$ are generators. This proves part ii). For p odd, the same argument proves part iii).

Obviously $\mathbb{Z}_2^\times$ is not topologically cyclic (because $(\mathbb{Z}/8\mathbb{Z})^\times$ is not cyclic). Since the groups Δ , $(\mathbb{Z}/q\mathbb{Z})^\times$ and $(1 + q\mathbb{Z}_p)$ are topologically cyclic, part ii) and part iii) imply part i). □

Interesting examples of topological generators

Now we bring examples of a generators of $\mathbb{Z}_p^\times/\{\pm 1\}$ which will become important later.

Lemma 19. *There exists an element $c \in \mathbb{Z}_p^\times$ which projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$ and which satisfies $c \in \mathbb{Z}$.*

Proof. Assume $p = 2$. Remember that $1 + q = 5$ is a generator of $1 + 4\mathbb{Z}_2$. Therefore 5 projects to a generator under the projection

$$\mathbb{Z}_2^\times \twoheadrightarrow \mathbb{Z}_2^\times/\{\pm 1\} \xrightarrow{\sim} \{0\} \times (1 + 4\mathbb{Z}_2)$$

Now assume p is odd. Remember that an element $1 + g \in 1 + p\mathbb{Z}_p$ is a generator if and only if $v_p(g) = 1$. Let

$$\xi = a_0 + a_1 p + \cdots \in \mu_{p-1} \subseteq \mathbb{Z}_p$$

be a $(p-1)$-th root of unity which generates μ_{p-1}. If $a_1 \neq 0$ then

$$a_0\xi^{-1} = a_0(a_0^{-1} - a_1a_0^{-2}p + \dots) \in 1 + p\mathbb{Z}_p$$

satisfies $v_p(a_0\xi^{-1} - 1) = 1$ and is therefore generator of $1 + p\mathbb{Z}_p$. Proposition 18 Part iii) imply that

$$\xi \cdot a_0\xi^{-1} = a_0 \in \mathbb{Z}$$

is a generator of $\mathbb{Z}_p^\times$ and therefore projected to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$. Thus we have to prove that there exists a generator

$$\xi = a_0 + a_1p + \dots \in \mu_{p-1} \subseteq \mathbb{Z}_p$$

of μ_{p-1}, which satisfies $a_1 \neq 0$. Now let

$$\hat{\xi} = b_0 + b_1p + \dots \in \mu_{p-1} \subseteq \mathbb{Z}_p$$

be a generator of μ_{p-1}. Assume $b_1 = 0$ (else we can stop). Let $\xi := -\hat{\xi}$. Since $p-1$ is even, the p-adic unit

$$\begin{aligned} \xi &= p - b_0 + (p - b_1 - 1)p + (p - b_2 - 1)p^2 + \dots \\ &= (p - b_0) + (p-1)p + \dots \end{aligned}$$

is also a generator and satisfies the demanded condition $p - 1 \neq 0$. □

Lemma 20. *There exists an element $c \in \mathbb{Z}_p^\times$ which projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$ and which satisfies*

$$b_0 = \frac{1}{2p^2}\log_p c^{p(p-1)} = 1.$$

Proof. It is a known fact that

$$\frac{1}{1-p} = 1 + p + p^2 + p^3 + \dots.$$

Note that therefore we have

$$\left|\frac{2p^2}{p(p-1)}\right|_p = \left|\frac{2p}{p-1}\right|_p = \left|\frac{2p}{1-p}\right|_p = |2p|_p = \begin{cases} p^{-1}, & \text{if } p \neq 2 \\ p^{-2}, & \text{if } p = 2 \end{cases} < p^{-1/(p-1)}$$

and since $exp_p(x) = 1 + x + \dots$ we have

$$v_p\left(\exp\left(\frac{2p}{p-1}\right) - 1\right) = v_p(2p + \dots) = \begin{cases} 1, & \text{if } p \neq 2 \\ 2, & \text{if } p = 2. \end{cases}$$

Lemma 15 states that

$$\hat{c} := \exp\frac{2p}{p-1}$$

is a generator of $(1 - q\mathbb{Z}_p)$. Let $g \in (\mathbb{Z}/q\mathbb{Z})^\times$ be an element which projects to a generator of Δ. We define

$$c := g\hat{c}.$$

Proposition 18 states that c projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$ and we have

$$\frac{1}{2p^2}\log_p(g\hat{c})^{p(p-1)} = \frac{1}{2p^2}\log_p(\hat{c})^{p(p-1)} = \frac{p(p-1)}{2p^2}\log_p\hat{c} = \frac{p-1}{2p}\log_p\left(\exp\frac{2p}{p-1}\right).$$

Since $\left|\frac{2p}{1-p}\right|_p < p^{-1/(p-1)}$ we have

$$\log_p\left(\exp\frac{2p}{p-1}\right) = \frac{2p}{p-1}.$$

□

2.2 Applications

This is a good moment to present and prove some propositions which will be needed later. We start with the formulation of some of the core problems this work is concerned with. Let

$$\tilde{q} := \varphi(q) = \begin{cases} p-1 & \text{if } p \text{ a odd prime} \\ 2 & \text{if } p = 2 \end{cases}.$$

Regard that $\tilde{q}$ is always even. In the later parts of this work it turns out, that for every $c \in \mathbb{Z}_p^\times$ which projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$, there exists an injection

$$\pi_0 E_\infty(MString, KO_p^\wedge) \hookrightarrow \bigoplus_{\substack{r\in\mathbb{Z}/\tilde{q} \\ r \text{ even}}} \mathbb{Z}_p[\![T]\!] =: \bigoplus_{r\in\mathbb{Z}/\tilde{q}}^{*} \mathbb{Z}_p[\![T]\!] \tag{21}$$

and one goal of this work is to determine the image of this map. The following definitions will play a major part in the solution of this problem

Definition 22. i) Let

$$\Gamma : \bigoplus_{r\in\mathbb{Z}/\tilde{q}}^{*} \mathbb{Z}_p[\![T]\!] \to \prod_{\substack{k\geq 4 \\ k \text{ even}}} \mathbb{Q}_p =: \prod_{k\geq 4}^{*} \mathbb{Q}_p$$

be defined by

$$(F_r)^*_{r\in\mathbb{Z}/\tilde{q}} \mapsto \Big(F_k\big((1+q)^k - 1\big)\Big)^*_{k\geq 4}.$$

ii) Let $c \in \mathbb{Z}_p^\times$ be an element which projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$. We say, an element

$$(z_k)^*_{k\geq 4} \in \mathrm{Im}(\Gamma)$$

satisfies Condition A for c if

$$z_k \in (1-c^k)\mathbb{Z}_p$$

for all even $k \geq 4$ which fulfil the property that $1 - c^k \in p\mathbb{Z}_p$. We denote the set of such sequences by $\mathbf{ConA}_c$.

Later it turns out that Γ is injective and that there exists an element

$$F_c^{Ber} = (F_{c,r}^{Ber})^*_{r\in\mathbb{Z}/\tilde{q}} \in \bigoplus_{r\in\mathbb{Z}/\tilde{q}}^{*} \mathbb{Z}_p[\![T]\!]$$

such that the image of map (21) is given by

$$F_c^{Ber} + \Gamma^{-1}(\mathbf{ConA}_c).$$

Let $c \in \mathbb{Z}_p^\times \cap \mathbb{Z}$ be an element which projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$ (the existence of such an element is proven in Lemma 19). Let

$$\mathbf{ConB}_c := \Big(\Gamma\left(F_c^{Ber}\right) + \mathbf{ConA}_c\Big) \cap \prod_{k \geq 4}^{*} \mathbb{Z}_{(p)}.$$

We will see that the image of the map

$$\pi_0 E_\infty(MString, KO_{(p)}) \hookrightarrow \pi_0 E_\infty(MString, KO_p^\wedge) \hookrightarrow \bigoplus_{r \in \mathbb{Z}/\tilde{q}}^{*} \mathbb{Z}_p[\![T]\!]$$

is given by $\Gamma^{-1}\Big(\mathbf{ConB}_c\Big)$. Therefore we have the following

Problem 23. *i) Let $c \in \mathbb{Z}_p^\times$ be an element which projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$. What is*

$$\Gamma^{-1}(\mathbf{ConA}_c)?$$

ii) Let $c \in \mathbb{Z}_p^\times \cap \mathbb{Z}$ be an element which projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$. What is

$$\Gamma^{-1}(\mathbf{ConB}_c)?$$

Part i) of Problem 23 is the easier one and will be handled in the rest of this section. Part ii) of Problem 23 is harder and still unsolved. There are only some information which will be presented later.

Condition A and power series

The first step is to split up Γ in its components. We have a disjoint union

$$2\mathbb{Z} = \bigcup_{\bar{r} \in \mathbb{Z}/\tilde{q},\ r \text{ even}} r + \tilde{q}\mathbb{Z}$$

and therefore a canonical bijection

$$\bigoplus_{r \in \mathbb{Z}/\tilde{q}}^{*} \left(\prod_{\substack{k \geq 4 \\ k \equiv r \bmod \tilde{q}}} \mathbb{Q}_p \right) \xrightarrow{\cong} \prod_{\substack{k \geq 4 \\ k \equiv 0 \bmod 2}} \mathbb{Q}_p = \prod_{k \geq 4}^{*} \mathbb{Q}_p$$

$$\big((x_{r,k})_k\big)_r \mapsto \left(\sum_r x_{r,k}\right)_k .$$

Definition 24. For every class $r \in \mathbb{Z}/\tilde{q}$ with r even we define the map

$$\Gamma_r : \mathbb{Z}_p[\![T]\!] \to \prod_{\substack{k \geq 4 \\ k \equiv r \bmod \tilde{q}}} \mathbb{Q}_p$$

by

$$F \mapsto \Big(F\big((1+q)^k - 1\big)\Big)_{k \geq 4,\ k \equiv r \bmod \tilde{q}} .$$

Now we can write

$$\Gamma : \bigoplus_{r\in\mathbb{Z}/\tilde{q}}^{*} \mathbb{Z}_p[\![T]\!] \xrightarrow{\oplus\Gamma_r} \bigoplus_{r\in\mathbb{Z}/\tilde{q}}^{*} \left(\prod_{\substack{k\geq 4\\ k\,\equiv\, r \bmod \tilde{q}}} \mathbb{Q}_p \right) \cong \prod_{k\geq 4}^{*} \mathbb{Q}_p.$$

Let $c \in \mathbb{Z}_p^\times$ be an element which projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$. The definition of Condition A leads to the following question.

For which even $k \geq 4$ is $1 - c^k \in p\mathbb{Z}_p$?

The answer is given by the following

Proposition 25. *Let $c \in \mathbb{Z}_p^\times$ be an element which projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$. The following conditions are equivalent:*

i) The positive integer k is even and $1 - c^k \in p\mathbb{Z}_p$.

ii) The positive integer k is an element of $\tilde{q}\mathbb{Z}$.

Proof. We defer the proof to the last paragraph of this subsection. □

Proposition 25 and the definition of $\mathbf{ConA}_c$ tells us, that

$$\Gamma\Big((F_r)^{*}_{r\in\mathbb{Z}/\tilde{q}}\Big) = \Big(F_k((1+q)^k - 1)\Big)^{*}_{k\geq 4} \in \mathbf{ConA}_c$$

if and only if

$$F_k((1+q)^k - 1) \in (1 - c^k)\mathbb{Z}_p$$

for all $k \in \tilde{q}\mathbb{Z}$ with $k \geq 4$, i.e. if and only if

$$F_0((1+q)^k - 1) \in (1 - c^k)\mathbb{Z}_p.$$

for all $k \in \tilde{q}\mathbb{Z}$ with $k \geq 4$. This lead to the following question.

Which

$$H \in \mathbb{Z}_p[\![T]\!]$$

satisfy the condition

$$H((1+q)^k - 1) \in (1 - c^k)\mathbb{Z}_p$$

for all $k \geq 4$ with $k \in \tilde{q}\mathbb{Z}$?

For the answer we need to proof the following

Proposition 26. *Let $c \in \mathbb{Z}_p^\times$ be an element which projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$. For all $k \in \tilde{q}\mathbb{Z}$, there exists elements $u_k \in \mathbb{Z}_p^\times$ such that*

$$(1+q)^k - 1 = u_k(c^k - 1).$$

Proof. Let $k \in \tilde{q}\mathbb{Z}$. We show that

$$c^k - 1 \equiv 0 \mod p^n$$

if and only if

$$(1+q)^k - 1 \equiv 0 \mod p^n$$

for all positive integers n. This imply $v_p(1-c^k) = v_p((1+q)^k - 1)$ and this imply the existence of an element $u_k \in \mathbb{Z}_p^\times$ which full fill the demanded condition. Remember that we have a commutative diagram

$$\begin{tikzcd} \mathbb{Z}_p^\times \arrow[r, two heads, "\langle . \rangle"] \arrow[d, "\pi"] & 1 + q\mathbb{Z}_p \arrow[d, "\mathrm{id}"] \\ \mathbb{Z}_p^\times/\{\pm 1\} \arrow[r, two heads, "\langle . \rangle"] & 1 + q\mathbb{Z}_p. \end{tikzcd}$$

Since πc is a generator and $\langle . \rangle$ is a surjective map of topological groups, we have that $\langle c \rangle = \langle \pi c \rangle$ is a generator of $1 + q\mathbb{Z}_p$. Since $(1+q)$ is also a generator of $1 + q\mathbb{Z}_p$ we have that

$$\langle c \rangle^k - 1 \equiv 0 \mod p^n$$

if and only if

$$(1+q)^k - 1 \equiv 0 \mod p^n$$

for all positive integers n. Since $k \in \tilde{q}\mathbb{Z}$ we have $\langle c \rangle^k = c^k$. □

Corollary 27. *Let $c \in \mathbb{Z}_p^\times$ be an element which projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$. A power series*

$$H(T) = \sum_{n \geq 0} \alpha_n T^n \in \mathbb{Z}_p[\![T]\!]$$

satisfy the condition

$$H((1+q)^k - 1) \in (1 - c^k)\mathbb{Z}_p$$

for all $k \in \tilde{q}\mathbb{Z}$ with $k \geq 4$, if and only if $H(0) = 0$.

Proof. Proposition 26 states that for every $k \in \tilde{q}\mathbb{Z}$ with $k \geq 4$ there exits an unit $u_k \in \mathbb{Z}_p^\times$ such that

$$\begin{aligned} H((1+q)^k - 1) = H(u_k(c^k - 1)) &= \sum_{n \geq 0} \alpha_n u_k^n (1 - c^k)^n \\ &= \alpha_0 + (1 - c^k) \sum_{n \geq 1} \alpha_n u_k^n (1 - c^k)^{n-1}. \end{aligned}$$

Therefore

$$H((1+q)^k - 1) \equiv 0 \mod (1 - c^k)$$

is equivalent to

$$\alpha_0 \equiv 0 \mod (1 - c^k)$$

for all $k \in \tilde{q}\mathbb{Z}$ with $k \geq 4$. This is equivalent to

$$\alpha_0 \in \bigcap_{k \in \tilde{q}\mathbb{Z},\, k \geq 4} (1 - c^k)\mathbb{Z}_p \subseteq \bigcap_{m \in \mathbb{N}} (1 - c^{(p-1)p^m})\mathbb{Z}_p \subseteq \bigcap_{m \in \mathbb{N}} p^{m+1}\mathbb{Z}_p = (0)$$

and this is equivalent to $H(0) = 0$. □

Now we can prove the main result of this subsection.

Proposition 28. *Let $c \in \mathbb{Z}_p^\times$ be an element which projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$. We have*

$$\Gamma^{-1}(\mathbf{ConA}_c) = \left\{ (F_r) \in \bigoplus_{r\in\mathbb{Z}/\tilde{q}}^{*} \mathbb{Z}_p[\![T]\!] \;\middle|\; F_0(0) = 0 \right\} = T\mathbb{Z}_p[\![T]\!] \oplus \bigoplus_{r\in(\mathbb{Z}/\tilde{q})-\{0\}}^{*} \mathbb{Z}_p[\![T]\!].$$

Proof. Remember that Proposition 25 and the definition of $\mathbf{ConA}_c$ tells us, that

$$\Gamma\big((F_r)^*_{r\in\mathbb{Z}/\tilde{q}}\big) = \Big(F_k((1+q)^k - 1)\Big)^*_{k\geq 4} \in \mathbf{ConA}_c$$

if and only if

$$F_k((1+q)^k - 1) = F_0((1+q)^k - 1) \in (1-c^k)\mathbb{Z}_p$$

for all $k \in \tilde{q}\mathbb{Z}$ with $k \geq 4$. Corollary 26 states that

$$F_0((1+q)^k - 1) \in (1-c^k)\mathbb{Z}_p$$

for all $k \in \tilde{q}\mathbb{Z}$ with $k \geq 4$ if and only if $F_0(0) = 0$. $\square$

Proof of Proposition 25

We fix an element c which projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$. Note that $1 - c^k \in p\mathbb{Z}_p$ is equivalent to $c^k \equiv 1 \mod p$.

First we proof the proposition for $p = 2$. Since $\varphi(4) = 2$ it is obvious that condition i) implies condition ii). Assume a positive integer k is an element of $\varphi(4)\mathbb{Z}$. Because c is a unit we have $c \equiv 1 \mod 2$, thus $c^k \equiv 1 \mod 2$.

Now let p be odd. We first show that condition ii) imply condition i). Assume the positive integer k is an element of $(p-1)\mathbb{Z}$ (this implies that k is even). Because c is a unit we know that $c^{p-1} \equiv 1 \mod p$. We know that

$$1 - c^k \in p\mathbb{Z}_p \;\Leftrightarrow c^k \equiv 1 \mod p.$$

Thus $c^k \equiv 1 \mod p$.

Now we assume condition i) is true, i.e. the positive integer k is even and $1 - c^k \in p\mathbb{Z}_p$. We have a commutative diagram

$$\begin{array}{ccc} \mathbb{Z}_p^\times & \xrightarrow{\pi_3} & (\mathbb{Z}/p\mathbb{Z})^\times \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_4} \\ \mathbb{Z}_p^\times/\{\pm 1\} & \xrightarrow{\pi_2} & (\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\} \end{array}$$

Since $\pi_1 c$ is a generator we know that $(\pi_2 \circ \pi_1)(c)$ is a generator. Since

$$(\pi_2 \circ \pi_1)(c)^k = \pi_4(\pi_3 c^k) = 1$$

and $(\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$ is a cyclic group of order $(p-1)/2$ we have $k \in \frac{p-1}{2}\mathbb{Z}$. We write

$$k = l\,\frac{p-1}{2} \;\text{ with }\; l \in \mathbb{Z}.$$

Now we lead the assumption $l \notin 2\mathbb{Z}$ to a contradiction, which proves $k \in (p-1)\mathbb{Z}$.

Assume $l \notin 2\mathbb{Z}$. Because k is even this implies that $(p-1)/2$ is even. Since $k \notin (p-1)\mathbb{Z}$ and $\pi_3 c^k = 1$ we know that $\pi_3 c$ is not a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. This is a contradiction to part i) of the following

Lemma 29. *Assume p is odd. Let n be a positive integer. Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ be an element which maps to a generator under the canonical projection*

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \to (\mathbb{Z}/p^n\mathbb{Z})^\times/\{\pm 1\}.$$

i) Assume $4|(p-1)$. Then a is a generator of $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

ii) Assume $4 \not|(p-1)$. Then either a or $-a$ is a generator of $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

Proof. The left hand side of the projection is a cyclic group of order $p^{n-1}(p-1)$. Thus the right hand side is a cyclic group of order $p^{n-1}\frac{p-1}{2}$. Let E be the set of generators of $(\mathbb{Z}/p\mathbb{Z})^\times$ and $\bar{E}$ the set of generators of $(\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$. Thus $a \in \pi^{-1}\bar{E}$. Because every generator projects to a generator we know that $E \subseteq \pi^{-1}\bar{E}$. Remember that for all positive integers x we have

$$\varphi(2x) = \begin{cases} \varphi(x), & \text{if } 2 \not| x \\ 2\varphi(x), & \text{if } 2|x \end{cases}$$

which imply

$$\varphi(p-1) = \begin{cases} \varphi(\frac{p-1}{2}), & \text{if } 2 \not| \frac{p-1}{2} \\ 2\varphi(\frac{p-1}{2}), & \text{if } 2|\frac{p-1}{2}. \end{cases}$$

Assume $4|(p-1)$. We now show that the E and $\pi^{-1}\bar{E}$ have the same cardinality. This imply $a \in E$. It obvious that $|\pi^{-1}\bar{E}| = 2|\bar{E}|$. Because $2|\frac{p-1}{2}$ we have

$$|E| = \varphi(p-1)\varphi(p^{n-1}) = 2\varphi(\frac{p-1}{2})\varphi(p^{n-1}) = 2|\bar{E}| = |\pi^{-1}\bar{E}|.$$

Assume $4 \not|(p-1)$. We have

$$|E| = \varphi(p-1)\varphi(p^{n-1}) = \varphi(\frac{p-1}{2})\varphi(p^{n-1}) = |\bar{E}| = \frac{1}{2}|\pi^{-1}\bar{E}|.$$

Assume both a and $-a$ are in $(\pi^{-1}\bar{E})-E$. Because of the last equation there exists a $b \in \pi^{-1}\bar{E}$ such that b and $-b$ are in E. But we have $(-b)^{p^{n-1}(p-1)/2} = (-1)b^{p^{n-1}(p-1)/2} = (-1)^2 = 1$ and so $-b$ is no generator. Thus either a or $-a$ is in E. This proves the claim of the Lemma. $\square$

3 Mahler expansions and p-adic measure theory

Let X be a compact and totally disconnected topological space. Important examples are $\mathbb{Z}_p$, $\mathbb{Z}_p^\times$ and $\mathbb{Z}_p^\times/\{\pm 1\}$. The set $\mathrm{cts}(X,\mathbb{Z}_p)$ of continuous p-adic functions on X carries a metric given by

$$\|f\| := \sup_{x\in X} |f(x)|_p = \max_{x\in X} |f(x)|_p.$$

A p-adic measures μ is a continuous $\mathbb{Z}_p$-module homomorphism

$$\mu : \mathrm{cts}(X,\mathbb{Z}_p) \to \mathbb{Z}_p.$$

The set of p-adic measures of X is denoted by $M(X,\mathbb{Z}_p)$. For $\mu \in M(X,\mathbb{Z}_p)$ and $f \in \mathrm{cts}(X,\mathbb{Z}_p)$ we use the notation

$$\int_X f d\mu := \mu(f).$$

The set $M(X,\mathbb{Z}_p)$ carries in a canonically way the structure of a $\mathbb{Z}_p$-module. In the later parts of this work X will mostly be $\mathbb{Z}_p^\times$ or $\mathbb{Z}_p^\times/\{\pm 1\}$.

Proposition 30. *Every $\mathbb{Z}_p$-module homomorphism between $\mathrm{cts}(X,\mathbb{Z}_p)$ and $\mathbb{Z}_p$ is continuous.*

Proof. Let $\varphi : \mathrm{cts}(X,\mathbb{Z}_p) \to \mathbb{Z}_p$ be a $\mathbb{Z}_p$-linear map. Because of the linearity is enough to check the continuity in $0 \in \mathrm{cts}(X,\mathbb{Z}_p)$. Assume the sequence $(f_n)_{n\geq 0} \in \mathrm{cts}(X,\mathbb{Z}_p)$ is a zero sequence, i.e.

$$\|f_n\| = \max_{x\in X} |f_n(x)|_p \to 0.$$

Let $\tilde{x} \in X$ be an element such that $|f(x)|_p = \|f_n\|$. We use the notation $M_n := v_p(\tilde{x})$. Then we have

$$f_n(x) \equiv 0 \mod p^{M_n}$$

for all $x \in X$ and the sequence (M_n) is unbounded. This imply the existence of a continuous function $g_n \in \mathrm{cts}(X,\mathbb{Z}_p)$ such that

$$f_n = p^{M_n} g_n.$$

Since $\left(p^{M_n}\right)_{n\geq 0}$ is a zero sequence we have that

$$(\varphi(f_n))_{n\geq 0} = \left(p^{M_n}\varphi(g_n)\right)_{n\geq 0}$$

is also a zero sequence. □

One of the main goals of this section is to determine the structure of

$$M(\mathbb{Z}_p^\times/\{\pm 1\},\mathbb{Z}_p).$$

Therefore we use the following

Lemma 31. *Let X, Y be compact and totally disconnected topological spaces. Let $h : X \to Y$ be a continuous map. We get a (module) homomorphism*

$$h^* : M(X,\mathbb{Z}_p) \to M(Y,\mathbb{Z}_p)$$

$$\mu \mapsto \nu$$

where ν is defined by

$$\int_Y f d\nu = \int_X f \circ h \, d\mu.$$

This map is an isomorphism if h is a homeomorphism.

Proof. The map

$$\nu : \mathrm{cts}(Y, \mathbb{Z}_p) \xrightarrow{h^*} \mathrm{cts}(X, \mathbb{Z}_p) \xrightarrow{\mu} \mathbb{Z}_p$$

is obviously $\mathbb{Z}_p$-linear. Since h_* is continuous we know that ν is continuous. If h is a homeomorphic then $(h^{-1})^*$ is obviously an inverse for h^*. □

From the last section we know that there is an isomorphism of topological groups (see Corollary 11)

$$\mathbb{Z}_p^\times/\{\pm 1\} \xrightarrow{\sim} \Delta \times \mathbb{Z}_p.$$

Thus we have an module isomorphism

$$M(\mathbb{Z}_p^\times/\{\pm 1\}, \mathbb{Z}_p) \xrightarrow{\sim} M(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p)$$

The right hand side of the isomorphism can be computed. Later we will see that

$$M(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p) = \bigoplus_{n=1}^{|\Delta|} M(\mathbb{Z}_p, \mathbb{Z}_p)$$

We know will investigate $M(\mathbb{Z}_p, \mathbb{Z}_p)$. Therefore we need some facts about $\mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p)$.

3.1 Continuous functions on the p-adic integers

Uniform convergence

Very important elements in the ring $\mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p)$ are the following functions.

Lemma 32. *For every integer n the assignment*

$$x \mapsto \binom{x}{n} := \begin{cases} \frac{1}{n!}\, x(x-1)\cdots(x-n+1) & n > 0 \\ 1 & n = 0 \\ 0 & n < 0 \end{cases}$$

gives an element in $\mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p)$.

Proof. Obviously the assignment $x \mapsto \binom{x}{n}$ gives an element in $\mathrm{cts}(\mathbb{Z}_p, \mathbb{Q}_p)$. We have to show that $\binom{x}{n} \in \mathbb{Z}_p$ for all $x \in \mathbb{Z}_p$. Let $x \in \mathbb{Z}_p$. Since $\mathbb{N}_0 \subseteq \mathbb{Z}_p$ is dense, there exists a sequence of positive integers (a_k) with $a_k \to x$. Since the assignment $x \mapsto \binom{x}{n}$ is continuous we have that $\binom{a_k}{n} \to \binom{x}{n}$. Because $\mathbb{Z}_p$ is compact and $\binom{a_k}{n} \in \mathbb{N}_0 \subseteq \mathbb{Z}_p$ we have that $\binom{x}{n} \in \mathbb{Z}_p$. □

Later we will see that these polynomials are some sort of generator of $\mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p)$. Therefore we need the following

Lemma 33. *Let $f_0, f_1, f_2, \dots \in \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p)$ be continuous functions and let $(a_n)_{n\geq 0} \in c_0(\mathbb{Z}_p)$ be a zero sequence. The function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ with*

$$f(x) = \sum_{n=0}^{\infty} a_n f_n(x) \quad \text{for } x \in \mathbb{Z}_p$$

is continuous. The series of continuous functions

$$\left(\sum_{n=0}^{N} a_n f_n \right)_{N \geq 0}$$

converges uniformly to f. In particular we have

$$\int_{\mathbb{Z}_p} \sum_{n=0}^{\infty} a_n f_n(x) d\mu(x) = \sum_{n=0}^{\infty} a_n \int_{\mathbb{Z}_p} f_n(x) d\mu(x)$$

for all measures $\mu \in M(\mathbb{Z}_p, \mathbb{Z}_p)$.

Proof. We only show that

$$\lim_{N\to\infty} \sum_{n=0}^{N} a_n f_n = f$$

in $\mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p)$, i.e. $\sum_{n=0}^{N} a_n f_n$ converges uniformly to f. The uniform convergence theorem then states that f is continuous. Regard that $|f(x)|_p \leq 1$ for all $x \in \mathbb{Z}_p$. We have

$$\left\| f - \sum_{n=0}^{N} a_n f_n \right\| = \left\| \sum_{n=N+1}^{\infty} a_n f_n \right\| = \max_{x\in\mathbb{Z}_p} \left| \sum_{n=N+1}^{\infty} a_n f_n(x) \right|_p \leq$$

$$\leq \max_{x\in\mathbb{Z}_p} \sum_{n=N+1}^{\infty} |a_n|_p |f_n|_p \leq \max_{x\in\mathbb{Z}_p} \sum_{n=N+1}^{\infty} |a_n|_p = \sum_{n=N+1}^{\infty} |a_n|_p$$

Since $\sum_{n\geq 0} |a_n|_p$ is convergent we have that

$$\lim_{N\to\infty} \sum_{n=N+1}^{\infty} |a_n|_p = 0.$$

□

Corollary 34. *Let $(a_n) \in c_0(\mathbb{Z}_p)$ be a zero sequence. The maps $f_1, f_2 : \mathbb{Z}_p \to \mathbb{Z}_p$ given by*

$$f_1(x) = \sum_{n\geq 0} a_n x^n$$

and

$$f_2(x) = \sum_{n\geq 0} a_n \binom{x}{n}$$

for $x \in \mathbb{Z}_p$ are continuous.

The difference operator

The operator

$$\Delta : \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p) \to \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p)$$

with

$$\Delta h(x) = h(x+1) - h(x)$$

defines an endomorphism of $\mathbb{Z}_p$-modules. The map

$$\varrho_n := \Delta^n(.)|_{x=0} : \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p) \xrightarrow{\Delta^n} \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p) \xrightarrow{f\mapsto f(0)} \mathbb{Z}_p$$

is $\mathbb{Z}_p$-linear and therefore an element of

$$\mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{cts}(\mathbb{Z}_p,\mathbb{Z}_p),\mathbb{Z}_p) = M(\mathbb{Z}_p,\mathbb{Z}_p).$$

Later we will show that $\varrho_0, \varrho_1, \ldots$ generates $M(\mathbb{Z}_p,\mathbb{Z}_p)$ as a $\mathbb{Z}_p$-module. We now collect some technical facts about Δ.

Lemma 35. *Let m, n be non-negative integers.*

i) For every constant function $f \in \mathrm{cts}(\mathbb{Z}_p,\mathbb{Z}_p)$ we have $\Delta f = 0$.

ii) If $m > n$ then $\Delta^m x^n = 0$.

iii) For all $m \geq 1$ and for all $f \in \mathrm{cts}(\mathbb{Z}_p,\mathbb{Z}_p)$ we have

$$\Delta^m(f(x)x) = x\Delta^m(f(x)) + m\Delta^{m-1}f(x+1).$$

iv) We have

$$\frac{1}{m!}\int_{\mathbb{Z}_p} x^n d\varrho_m(x) = \frac{\Delta^m x^n|_{x=0}}{m!} \in \mathbb{Z}_p.$$

v) We have

$$\Delta^m \binom{x}{n} = \binom{x}{n-m}.$$

In particular we have

$$\int_{\mathbb{Z}_p} \binom{x}{n} d\varrho_m(x) = \Delta^m \binom{x}{n}\Big|_{x=0} = \begin{cases} 1 & m = n \\ 0 & m \neq n \end{cases}.$$

Proof. i) This is obvious.

ii) We use an induction on n. Part i) tells us that the statement is true for $n = 0$. Assume the statement holds for all non-negative integers $\leq n$. Let $m > n+1$. Then

$$\Delta^m x^{n+1} = \Delta^{m-1}((x+1)^{n+1} - x^{n+1})$$
$$= \Delta^{m-1}\sum_{k=0}^{n}\binom{n+1}{k}x^k = \sum_{k=0}^{n}\binom{n+1}{k}\Delta^{m-1}x^k.$$

Since $m-1 > n \geq k$ the induction hypothesis imply that $\Delta^{m-1}x^k = 0$ for all m and $k \in \{0,\ldots,n\}$ and therefore the right hand side of the equation is 0.

iii) We use an induction on m. Let $m = 1$. Then

$$\Delta(f(x)x) = f(x+1)(x+1) - f(x)x$$
$$= f(x+1)x - f(x)x + f(x+1) = x\Delta f(x) + f(x+1).$$

Assume the statement holds for all positive integers $\leq m$. Then we have

$$\Delta\Delta^m(f(x)x) = \Delta\Big(x\Delta^m(f(x)) + m\Delta^{m-1}f(x+1)\Big)$$
$$= \Delta\Big(x\Delta^m(f(x))\Big) + m\Delta^1 f(x+1)$$
$$= \Big(x\Delta^{m+1}(f(x)) + \Delta^m f(x+1)\Big) + m\Delta^m f(x+1)$$
$$= x\Delta^{m+1}(f(x)) + (m+1)\Delta^m f(x+1).$$

iv) If $m = 0$ the statement is obviously true. Assume $m > 0$. We use an induction on n. The statement is obviously true for $n = 0$. Assume the statement holds for all non-negative integers $\leq n$. Then Part iii) imply

$$\Delta^m x^{n+1}|_{x=0} = \Delta^m (x^n x)|_{x=0} = x\Delta^m(x^n)|_{x=0} + m\Delta^{m-1}(x+1)^n|_{x=0}$$
$$= m\left(\Delta^{m-1}\sum_{k=0}^{n}\binom{n}{k}x^k\right)\Big|_{x=0} = m\sum_{k=0}^{n}\binom{n}{k}\Delta^{m-1}x^k|_{x=0}.$$

The induction hypothesis states that $\Delta^{m-1}x^k|_{x=0} = (m-1)!z_k$ for an element $z_k \in \mathbb{Z}_p$, thus the right hand side of the equation equals

$$m(m-1)!\sum_{k=0}^{n}\binom{n}{k}z_k \in \mathbb{Z}_p.$$

v) We use an induction on m. The statement is obviously true for $m = 0$. Assume the statement holds for all non-negative integers $\leq m$. Then

$$\Delta^{m+1}\binom{x}{n} = \Delta\binom{x}{n-m} = \binom{x+1}{n-m} - \binom{x}{n-m}$$
$$= \binom{x}{n-m-1} + \binom{x}{n-m} - \binom{x}{n-m} = \binom{x}{n-(m+1)}.$$

□

Lemma 36. *For every function $h \in \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p)$ we have*

$$\int_{\mathbb{Z}_p} h\, d\varrho_n = \Delta^n h(0) = \sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}h(i).$$

Proof. We use induction on n. For $n = 0$ the equation is obviously true. Assume the equation is true for a non negative integer n and for all $h \in \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p)$. Then we have

$$\Delta^{n+1}h(0) = \Delta^{n+1}h(x)|_{x=0} = \Delta^n h(x+1)|_{x=0} - \Delta^n h(x)|_{x=0}.$$

Using the induction hypothesis we have

$$\Delta^n h(x+1)|_{x=0} - \Delta^n h(x)|_{x=0} = \left(\sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}h(i+1)\right) - \left(\sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}h(i)\right)$$
$$= \left(\sum_{i=1}^{n+1}(-1)^{n-i-1}\binom{n}{i-1}h(i)\right) + \left(\sum_{i=0}^{n}(-1)^{n-i+1}\binom{n}{i}h(i)\right)$$
$$= h(n+1) + \left(\sum_{i=1}^{n}(-1)^{n-i+1}\left(\binom{n}{i-1} + \binom{n}{i}\right)h(i)\right) + (-1)^{n+1}h(0)$$
$$= \sum_{i=0}^{n+1}(-1)^{n-i+1}\binom{n+1}{i}h(i).$$

□

The Theorem of Mahler

Theorem 37 (Mahler)**.** *Let $c_0(\mathbb{Z}_p)$ be the group of zero-sequences in $\mathbb{Z}_p$. The map*

$$c_0(\mathbb{Z}_p) \to \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p)$$

$$(a_n) \mapsto \sum_{n\geq 0} a_n \binom{x}{n}$$

is a $\mathbb{Z}_p$-module isomorphism. The inverse isomorphism is given by

$$f \mapsto (\Delta^n f(0))_{n\geq 0} = \left(\int_{\mathbb{Z}_p} f \, d\varrho_n\right)_{n\geq 0}.$$

Sketch of proof. For the complete proof see for example [Lan, Chapter 4, Theorem 1.3]. The hard part is two show that $(\Delta^n f(0))_{n\geq 0}$ is a zero sequence. Then it has to been shown that

$$f(k) = \sum_{n\geq 0} (\Delta^n f(0)) \binom{k}{n}$$

for all non-negative integers k. Because of the density of $\mathbb{N}_0 \subseteq \mathbb{Z}_p$ we then get

$$f(x) = \sum_{n\geq 0} (\Delta^n f(0)) \binom{x}{n}$$

by continuity. After that it has to be shown that

$$\Delta^n \left(\sum_{m\geq 0} a_m \binom{x}{m} \right) (0) = a_n$$

for all $n \geq 0$. It is obvious that the maps are $\mathbb{Z}_p$-module homomorphisms. Therefore the two maps a inverse homomorphisms. □

Example 38. Remember that a^x is defined to be $\exp(x \log_p a)$ if $a - 1 \in p\mathbb{Z}_p$. Let $b = a - 1$. We show that

$$(1 + b)^x = \sum_{n\geq 0} \binom{x}{n} b^n$$

for all $x \in \mathbb{Z}_p$. Assume x is a non-negative integer. It is obvious that

$$(1 + b)^x = \sum_{n\geq 0} \binom{x}{n} b^n.$$

Because $\mathbb{N}_0$ is dense in $\mathbb{Z}_p$ the equation is true for all $x \in \mathbb{Z}_p$.

Analytic functions on the p-adic integers I

This is a good opportunity to prepare some results needed later to prove Theorem C. The following two paragraphs will help us to attack part ii) of Problem 23.

Let $x, a_0, a_1, a_2, \dots \in \mathbb{Z}_p$. Remember that the series $\sum a_n x^n$ is absolute convergent if and only if the sequence $(a_n x^n)$ is a zero sequence and because $|a_n|_p \leq 1$ this is fulfilled if and only if (x^n) is a zero sequence. Since (p^n) is an zero sequence and $|x|_p \leq 1$ we have that $(p^n x^n)$ is a zero sequence. Therefore there is an well-defined injective map

$$\kappa_1 : \mathbb{Z}_p[\![T]\!] \hookrightarrow \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p) \xrightarrow{\sim} c_0(\mathbb{Z}_p)$$

$$F = \sum a_m T^m \mapsto \big(x \mapsto F(px)\big) \mapsto \left(\int_{\mathbb{Z}_p} F(px)\, d\varrho_n(x) \right)_{n\geq 0} = \left(\sum_{m\geq 0} a_m p^m \int_{\mathbb{Z}_p} x^m \, d\varrho_n(x) \right)_{n\geq 0}.$$

The right hand map is an isomorphism given by the Theorem of Mahler. Let $\mathbf{X}_1$ be the image of κ_1. Now we have the following

Problem 39. *What is the image $\mathbf{X}_1$ of κ_1?*

This problem can be solved. The next proposition is a modification of a result from Lazard found in [Laz, page 79].

Proposition 40. *A sequence $(b_n)_{n\geq 0} \in c_0(\mathbb{Z}_p)$ is in the image of the map κ_1 if and only if*

$$\frac{b_n}{n!\, p^n} \in \mathbb{Z}_p$$

for all $n \geq 0$.

Proof. Let (b_n) be a sequence in $c_0(\mathbb{Z}_p)$ and $f \in \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p)$ be the corresponding function. The Theorem of Mahler states that

$$f = \sum_{n\geq 0} b_n \binom{x}{n}.$$

For each $n \geq 1$ there exists integers $l_{1,n}, \ldots, l_{n,n}$ such that

$$n! \binom{x}{n} = x(x-1)\ldots(x-n+1) = \sum_{k=1}^{n} l_{k,n} x^k.$$

Assume $b_n = n! p^n \, \hat{b}_n$, where $\hat{b}_n \in \mathbb{Z}_p$. This imply

$$f = b_0 + \sum_{n\geq 1} b_n \binom{x}{n} = b_0 + \sum_{n\geq 1} \left(\hat{b}_n p^n \sum_{k=1}^{n} l_{k,n} x^k \right).$$

Regard that

$$\sum_{n\geq 1} \sum_{k=1}^{n} s_{n,k} = \sum_{\substack{(k,n)\in\mathbb{N}^2 \\ k\leq n}} s_{n,k} = \sum_{k\geq 1} \sum_{n\geq k} s_{n,k} = \sum_{n\geq 1} \sum_{k\geq n} s_{k,n}$$

if the $s_{n,k} \in \mathbb{Z}_p$ are chosen in such way that every thing is convergent. Thus

$$f = b_0 + \sum_{n\geq 1} \sum_{k=1}^{n} \left(\hat{b}_n p^n l_{k,n} \right) x^k = b_0 + \sum_{n\geq 1} \sum_{k\geq n} \left(\hat{b}_k p^k l_{n,k} \right) x^n =$$

$$= b_0 + \sum_{n\geq 1} \left(\sum_{k\geq 0} \hat{b}_{k+n} p^{k+n} l_{n,k+n} \right) x^n = b_0 + \sum_{n\geq 1} a_n p^n x^n$$

where

$$a_n := \sum_{k\geq 0} l_{n,k+n}\hat{b}_{k+n}p^k$$

is a convergent series since p^k is a zero sequence. Thus (b_n) is the image of the power series

$$b_0 + \sum_{n\geq 1} a_n T^n \in \mathbb{Z}_p[\![T]\!]$$

under the map κ_1.

Assume in return that there exists a series $\sum_{m\geq 0} a_m T^m \in \mathbb{Z}_p[\![T]\!]$ such that

$$f(x) = \sum_{m\geq 0} a_m p^m x^m.$$

Then b_n is defined to be

$$\int_{\mathbb{Z}_p} f \, d\varrho_n = \int_{\mathbb{Z}_p} \sum_{m\geq 0} a_m p^m x^m \, d\varrho_n(x) = \sum_{m\geq 0} a_m p^m \int_{\mathbb{Z}_p} x^m \, d\varrho_n(x).$$

With Part ii) and Part iv) of Lemma 35 we get

$$\int_{\mathbb{Z}_p} x^m \, d\varrho_n = \begin{cases} n!\, s_{m,n}, & m \geq n \\ 0, & m < n \end{cases}$$

where $s_{m,n} \in \mathbb{Z}_p$. Thus we have

$$b_n = \sum_{m\geq 0} a_m p^m \int_{\mathbb{Z}_p} x^m \, d\varrho_n(x) = \sum_{m\geq n} a_m p^m n! s_{m,n} = n! p^n \sum_{m\geq 0} a_{m+n} p^m s_{m+n,n}$$

and this imply

$$\frac{b_n}{n!p^n} \in \mathbb{Z}_p.$$

$\square$

Analytic functions on the p-adic integers II

Remember that

$$\tilde{q} := \begin{cases} p-1 & \text{if } p \text{ a odd prime} \\ 2 & \text{if } p = 2 \end{cases}$$

For a non-negative even integer u we define a continuous function

$$\gamma_u : \mathbb{Z}_p \to \mathbb{Z}_p$$

$$x \mapsto (1+q)^{\tilde{q}x+u} - 1.$$

Regard that $v_p(\gamma_u(x)) > 0$ for all $x \in \mathbb{Z}_p$ and therefore $(\gamma_u(x)^n)_{n\geq 0}$ is a zero sequence. Thus the map

$$\kappa_2 := \kappa_{2,u} : \mathbb{Z}_p[\![T]\!] \to \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p) \xrightarrow{\sim} c_0(\mathbb{Z}_p)$$

$$F = \sum a_m T^m \mapsto \big(x \mapsto F(\gamma_r(x))\big) \mapsto \left(\int_{\mathbb{Z}_p} F(\gamma_u(x))\, d\varrho_n(x)\right)_{n\geq 0}$$

$$= \left(\sum_{m \geq 0} a_m \int_{\mathbb{Z}_p} \gamma_u^m(x) \, d\varrho_n(x) \right)_{n \geq 0}.$$

is well-defined. Let $\mathbf{X}_2 := \mathbf{X}_{2,u}$ be the image of κ_2. First prove that κ_2 is injective, which is an immediate consequence of the following

Lemma 41. *Let u be a non-negative even integer.*

i) The map

$$\gamma_u : \mathbb{Z}_p \to q\mathbb{Z}_p$$
$$x \mapsto (1+q)^{\tilde{q}x+u} - 1.$$

is a well-defined isomorphism of topological spaces.

ii) The map

$$\mathbb{Z}_p[\![T]\!] \to \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p)$$
$$F \mapsto F(\gamma_u(x))$$

is injective.

Proof. i) Regard that $\tilde{q} \in \mathbb{Z}_p$ is either a unit (for p odd) or 2 (for p=2). In each case the even integer u is an element of $\tilde{q}\mathbb{Z}_p$. Regard that $(1+q)^{\tilde{q}} \in 1 + q\mathbb{Z}_p$ and therefore the map

$$\mathbb{Z}_p \overset{(1+q)^{\tilde{q}\bullet}}{\longrightarrow} 1 + q\mathbb{Z}_p$$

is an isomorphism of topological groups (see Corollary 5). Thus

$$\tilde{q}\mathbb{Z}_p \overset{(1+q)^{\bullet}}{\longrightarrow} 1 + q\mathbb{Z}_p$$

is a topological isomorphism. Now the map γ_u can be described as a composition of isomorphisms of topological groups

$$\mathbb{Z}_p \xrightarrow{\cdot\tilde{q}} \tilde{q}\mathbb{Z}_p \xrightarrow{+u} \tilde{q}\mathbb{Z}_p \overset{(1+q)^{\bullet}}{\longrightarrow} 1 + q\mathbb{Z}_p \xrightarrow{-1} q\mathbb{Z}_p.$$

ii) Assume

$$F(\gamma_u(x)) = \hat{F}(\gamma_u(x))$$

for all $x \in \mathbb{Z}_p$ with $F(T), \hat{F}(T)$ power series. With Part i) we have

$$F(qy) = \hat{F}(qy)$$

for all $y \in \mathbb{Z}_p$, i.e. $F(qT) = \hat{F}(qT)$ in $\mathbb{Z}_p[\![T]\!]$ and this imply $F = \hat{F}$.

□

Again we have the following

Problem 42. *What is the image $\mathbf{X}_2$ of κ_2?*

This time the problem is much harder and still open. For readers who are interested in solving this problem we now collect some facts which are maybe helpful.

Lemma 43. *Let $b \in q\mathbb{Z}_p$ and n be a non-negative integer. Then*

$$\int_{\mathbb{Z}_p} (1+b)^x \, d\varrho_n(x) = b^n.$$

Proof. Example 38 states that

$$(1+b)^x = \sum_{i \geq 0} \binom{x}{i} b^i.$$

The claim is now implied by Part v) of Lemma 35, which states that

$$\int_{\mathbb{Z}_p} \binom{x}{i} \, d\varrho_n(x) = \begin{cases} 1 & i = n \\ 0 & \text{else} \end{cases}.$$

□

Proposition 44. *Let u be a non-negative even integer. For all non-negative integers n, m we have*

$$\int_{\mathbb{Z}_p} \gamma_u^m(x) \, d\varrho_n(x) = \sum_{i=0}^{m} \binom{m}{i} (-1)^{m-i} (1+q)^{iu} \Big((1+q)^{\tilde{q}i} - 1 \Big)^n.$$

Proof. We have

$$\gamma_u^m(x) = \Big((1+q)^{\tilde{q}x+u} - 1 \Big)^m = \sum_{i=0}^{m} \binom{m}{i} (-1)^{m-i} (1+q)^{\tilde{q}ix+iu}$$

and further

$$(1+q)^{\tilde{q}ix} = \left(1 + \sum_{j=1}^{\tilde{q}i} \binom{\tilde{q}i}{j} q^j \right)^x$$

for $i = 0, \ldots, m$. With the last Lemma we have

$$\int_{\mathbb{Z}_p} (1+q)^{\tilde{q}ix+iu} \, d\varrho_n(x) = (1+q)^{iu} \int_{\mathbb{Z}_p} (1+q)^{\tilde{q}ix} \, d\varrho_n(x)$$

$$= (1+q)^{iu} \left(\sum_{j=1}^{\tilde{q}i} \binom{\tilde{q}i}{j} q^j \right)^n = (1+q)^{iu} \Big((1+q)^{\tilde{q}i} - 1 \Big)^n.$$

All together we get

$$\int_{\mathbb{Z}_p} \gamma_u^m(x) \, d\varrho_n(x) = \sum_{i=0}^{m} \binom{m}{i} (-1)^{m-i} (1+q)^{iu} \Big((1+q)^{\tilde{q}i} - 1 \Big)^n.$$

□

Corollary 45. *Let u be a non-negative even integer. Let n, m be non-negative integers.*

i) We have

$$\int_{\mathbb{Z}_p} \gamma_u^m(x) \, d\varrho_n(x) = \int_{\mathbb{Z}_p} (1+q)^{ux} \Big((1+q)^{\tilde{q}x} - 1 \Big)^n d\varrho_m(x)$$

$$= \int_{\mathbb{Z}_p} (1+q)^{ux} \gamma_0^n(x) \, d\varrho_m(x).$$

ii) We have

$$\frac{1}{q^n}\int_{\mathbb{Z}_p} \gamma_u^m(x)\, d\varrho_n(x) \in \mathbb{Z}_p.$$

Proof. i) This is an immediate consequence of Lemma 36 which states that

$$\int h\, d\varrho_m = \sum_{i=0}^{m} \binom{m}{i}(-1)^{m-i} h(i)$$

for all continuous function h.

ii) This follows immediately from Part I) because $v_p(\gamma_0(x)) \geq v_p(q)$, i.e.

$$\frac{\gamma_0^n(x)}{q^n} \in \mathbb{Z}_p$$

for all $x \in \mathbb{Z}_p$.

□

3.2 Measures on $\mathbb{Z}_p$

We start by giving very important examples of measures in $M(\mathbb{Z}_p, \mathbb{Z}_p)$.

Lemma 46. *For every series $H(T) = \sum_{n\geq 0} b_n T^n \in \mathbb{Z}_p[\![T]\!]$ the map*

$$\nu_H : \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p) \to \mathbb{Z}_p$$

$$f \mapsto \sum_{n\geq 0} b_n \int_{\mathbb{Z}_p} f\, d\varrho_n.$$

defines a measure in $M(\mathbb{Z}_p, \mathbb{Z}_p)$.

Proof. This is obvious since ϱ_n is $\mathbb{Z}_p$-linear for all $n \geq 0$ and the Theorem of Mahler states that $(\int f\, d\varrho_n)_n$ is a zero sequence. □

For $n \geq 0$ and a measure $\mu \in M(\mathbb{Z}_p, \mathbb{Z}_p)$ we write

$$b_n(\mu) = \int_{\mathbb{Z}_p} \binom{x}{n} d\mu(x).$$

Proposition 47. *There is a $\mathbb{Z}_p$-module isomorphism*

$$F_\bullet : M(\mathbb{Z}_p, \mathbb{Z}_p) \xrightarrow{\sim} \mathbb{Z}_p^{\mathbb{N}} \cong \mathbb{Z}_p[\![T]\!]$$

$$\mu \mapsto F_\mu(T) := \sum_{n\geq 0} b_n(\mu) T^n$$

The assignment $H \mapsto \nu_H$ described in Lemma 46 is the inverse module isomorphism of $F_\bullet$. The $\mathbb{Z}_p$-algebra structure of $\mathbb{Z}_p[\![T]\!]$ induces via $F_\bullet$ an $\mathbb{Z}_p$-algebra structure on $M(\mathbb{Z}_p, \mathbb{Z}_p)$.

Proof. It is obvious that $F_\bullet$ and the map in iii) are $\mathbb{Z}_p$-module homomorphisms. We now show that $\nu_{F_\mu} = \mu$ and $F_{\nu_F} = F$. Using the Theorem of Mahler we get

$$\int_{\mathbb{Z}_p} f d\mu(x) = \int_{\mathbb{Z}_p} \sum_{n\geq 0} \left(\int_{\mathbb{Z}_p} f \, d\varrho_n \right) \binom{x}{n} d\mu(x).$$

Lemma 33 states that we can change summation and integration, thus the right hand side equals

$$\sum_{n\geq 0} \left(\int_{\mathbb{Z}_p} f \, d\varrho_n \right) \left(\int_{\mathbb{Z}_p} \binom{x}{n} d\mu(x) \right) = \sum_{n\geq 0} b_n(\mu) \int_{\mathbb{Z}_p} f \, d\varrho_n = \int_{\mathbb{Z}_p} f d\nu_{F_\mu}(x)$$

where the last equation is implied by Lemma 46. Thus $\nu_{F_\mu} = \mu$.

Let $F(t) = \sum b_n T^n$. Using Lemma 46 again we get

$$b_n(\nu_F) = \int_{\mathbb{Z}_p} \binom{x}{n} d\nu_F = \sum_{m\geq 0} b_m \int_{\mathbb{Z}_p} \binom{x}{n} \, d\varrho_m(x).$$

Part v) of Lemma 35 states that

$$\int_{\mathbb{Z}_p} \binom{x}{n} \, d\varrho_m(x) = \begin{cases} 1 & m = n \\ 0 & \text{else} \end{cases} .$$

Therefore $b_n(\nu_F) = b_n$ which implies

$$F_{\nu_F} = F.$$

□

We will describe now the multiplication on $M(\mathbb{Z}_p, \mathbb{Z}_p)$ induced by $F_\bullet$. Let $\mu, \nu \in M(\mathbb{Z}_p, \mathbb{Z}_p)$. Proposition 47 imply that the product

$$\mu * \nu := (F_\bullet)^{-1}(F_\mu F_\nu) = (F_\bullet)^{-1} \left(\sum_{n\geq 0} \left(\sum_{i+j=n} b_i(\mu) b_j(\nu) \right) T^n \right)$$

defines a multiplication on $M(\mathbb{Z}_p, \mathbb{Z}_p)$.

Lemma 48. *For all $x, t \in \mathbb{Z}_p$ and for all non-negative integers n we have*

$$\binom{x+t}{n} = \sum_{i+j=n} \binom{x}{i} \binom{t}{j}$$

Proof. The maps

$$(x,t) \to \binom{x+t}{n}$$

and

$$(x,t) \to \sum_{i+j=n} \binom{x}{i} \binom{t}{j}$$

are polynomial and therefore elements of $\mathrm{cts}(\mathbb{Z}_p \times \mathbb{Z}_p, \mathbb{Z}_p)$. Remember that for all non-negative integers r, s the equation

$$\binom{r+s}{n} = \sum_{i+j=n} \binom{r}{i} \binom{s}{j}$$

is true. Because $\mathbb{N}_0 \times \mathbb{N}_0 \subseteq \mathbb{Z}_p \times \mathbb{Z}_p$ is dense the statement of the Lemma is true by continuity. □

Corollary 49. *Let $f \in \operatorname{cts}(\mathbb{Z}_p, \mathbb{Z}_p)$ and $\mu \in M(\mathbb{Z}_p, \mathbb{Z}_p)$ The assignment*

$$x \mapsto \int_{\mathbb{Z}_p} f(x+t)d\mu(t)$$

defines a continuous function in $\operatorname{cts}(\mathbb{Z}_p, \mathbb{Z}_p)$.

Proof. Let n be a non-negative integer. Consider the map

$$\varphi_n : \mathbb{Z}_p \to \mathbb{Z}_p$$
$$x \mapsto \int_{\mathbb{Z}_p} \binom{x+t}{n} d\mu(t)$$

We have

$$\int_{\mathbb{Z}_p} \binom{x+t}{n} dt = \int_{\mathbb{Z}_p} \sum_{i+j=n} \binom{x}{i}\binom{t}{j} d\mu(t) = \sum_{i+j=n} \binom{x}{i} \int_{\mathbb{Z}_p} \binom{t}{j} d\mu(t) = \sum_{i+j=n} \binom{x}{i} b_j(\mu).$$

As sum of continuous functions, the map φ_n is also continuous. There is a zero sequence (a_n) such that

$$f = \sum_{n \geq 0} a_n \binom{x}{n}.$$

Using Lemma 33 all the way we get that the assignment

$$x \mapsto \int_{\mathbb{Z}_p} f(x+t)d\mu(t) = \int_{\mathbb{Z}_p} \sum_{n\geq 0} a_n \binom{x+t}{n} d\mu(t)$$

$$= \sum_{n\geq 0} a_n \int_{\mathbb{Z}_p} \binom{x+t}{n} d\mu(t) = \sum_{n \geq 0} a_n \varphi_n(x)$$

is continuous. □

Proposition 50. *For all measures $\mu, \nu \in M(\mathbb{Z}_p, \mathbb{Z}_p)$ and all continuous functions $f \in \operatorname{cts}(\mathbb{Z}_p, \mathbb{Z}_p)$ we have*

$$\int_{\mathbb{Z}_p} f(x)d(\mu * \nu)(x) = \int_{\mathbb{Z}_p}\int_{\mathbb{Z}_p} f(x+t)d\mu(x)d\nu(t).$$

Proof. The value $(\mu * \nu)(f)$ is defined to be

$$\left[(F_\bullet)^{-1} \left(\sum_{n\geq 0} \left(\sum_{i+j=n} b_i(\mu) b_j(\nu) \right) T^n \right) \right] (f)$$

Lemma 46 imply that

$$\int_{\mathbb{Z}_p} f(x)d(\mu * \nu)(x) = \sum_{n\geq 0} \sum_{i+j=n} b_i(\mu)b_j(\nu) \int_{\mathbb{Z}_p} f \, d\varrho_n.$$

The Theorem of Mahler states that

$$f = \sum_{n \geq 0} \binom{x}{n} \int_{\mathbb{Z}_p} f \, d\varrho_n.$$

Therefore

$$\int_{\mathbb{Z}_p}\int_{\mathbb{Z}_p} f(x+t)d\mu(x)d\nu(t) = \sum_{n\geq 0}\int_{\mathbb{Z}_p}\int_{\mathbb{Z}_p}\binom{x+t}{n}d\mu(x)d\nu(t)\int_{\mathbb{Z}_p} f\,d\varrho_n.$$

With Lemma 48 we have

$$\int_{\mathbb{Z}_p}\int_{\mathbb{Z}_p}\binom{x+t}{n}d\mu(x)d\nu(t) = \sum_{i+j=n}\int_{\mathbb{Z}_p}\int_{\mathbb{Z}_p}\binom{x}{i}\binom{t}{j}d\mu(x)d\nu(t)$$

$$= \sum_{i+j=n}\int_{\mathbb{Z}_p}\binom{x}{i}d\mu(x)\int_{\mathbb{Z}_p}\binom{t}{j}d\nu(t) = \sum_{i+j=n} b_i(\mu)b_j(\nu).$$

This proves the proposition. □

A $\mathbb{Z}_p$-group action

Now we have that $M(\mathbb{Z}_p,\mathbb{Z}_p)$ carries the structure of a $\mathbb{Z}_p$-algebra. But there is additional structure.

Lemma 51. *The map*

$$\mathbb{Z}_p \times M(\mathbb{Z}_p,\mathbb{Z}_p) \to M(\mathbb{Z}_p,\mathbb{Z}_p)$$

$$(\lambda,\mu) \mapsto \lambda\odot\mu$$

where $\lambda\odot\mu$ is defined by

$$\int_G f d\lambda\odot\mu = \int_G f(\lambda+x)d\mu(x)$$

is a group action.

Proof. The map

$$\lambda\mu : \mathrm{cts}(\mathbb{Z}_p,\mathbb{Z}_p) \to \mathrm{cts}(\mathbb{Z}_p,\mathbb{Z}_p) \xrightarrow{\mu} \mathbb{Z}_p$$

$$f \mapsto f\circ(+\lambda) \mapsto \int_G f(\lambda+x)d\mu(x)$$

is obviously $\mathbb{Z}_p$-linear. Since $(+\lambda)$ and μ are continuous we have that $\lambda\mu$ is a measure. □

We can also give $\mathbb{Z}_p[\![T]\!]$ the structure of a $\mathbb{Z}_p$-set in such a way, that $F_\bullet$ is $\mathbb{Z}_p$-equivariant.

Lemma 52. *The map*

$$\mathbb{Z}_p \times \mathbb{Z}_p[\![T]\!] \to \mathbb{Z}_p[\![T]\!]$$

$$(\lambda, F(T)) \mapsto \lambda\odot F(T) := (1+T)^\lambda \cdot F(T)$$

is a group action. The isomorphism of $\mathbb{Z}_p$-algebras

$$F_\bullet : M(\mathbb{Z}_p,\mathbb{Z}_p) \xrightarrow{\sim} \mathbb{Z}_p[\![T]\!]$$

is $\mathbb{Z}_p$-equivariant.

Proof. Obviously we have $0 \odot F(T) = F(T)$ and $\kappa \odot (\lambda \odot F(T)) = (\kappa + \lambda) \odot F(T)$. In Example 38 we showed that

$$(1+T)^\lambda = \sum_{n \geq 0} \binom{\lambda}{n} T^n \in \mathbb{Z}_p[\![T]\!].$$

Remember that together with Lemma 48 we have

$$b_n(\lambda \odot \mu) = \int_{\mathbb{Z}_p} \binom{x}{n} d(\lambda \odot \mu)(x) = \int_{\mathbb{Z}_p} \binom{x+\lambda}{n} d\mu(x)$$

$$= \int_{\mathbb{Z}_p} \sum_{i+j=n} \binom{x}{i}\binom{\lambda}{j} d\mu(x) = \sum_{i+j=n} \binom{\lambda}{j} b_i(\mu).$$

for all $n \geq 0$. This imply

$$F_{\lambda \odot \mu}(T) = \sum_{n \geq 0} b_n(\lambda \odot \mu) T^n = \sum_{n \geq 0} \left(\sum_{i+j=n} \binom{\lambda}{j} b_i(\mu) \right) T^n$$

$$= \left(\sum_{n \geq 0} \binom{\lambda}{n} T^n \right) \left(\sum_{n \geq 0} b_n(\mu) T^n \right) = (1+T)^\lambda F_\mu = \lambda \odot F_\mu.$$

□

The Quotient of the action on $\mathbb{Z}_p[\![T]\!]$

With $\sim_{\mathbb{Z}_p}$ we denote the equivalence relation on $\mathbb{Z}_p[\![T]\!]$ induced by the $\mathbb{Z}_p$-action, i.e. $F \sim_{\mathbb{Z}_p} \tilde{F}$ if and only if there exists a $\lambda \in \mathbb{Z}_p$ such that $F = \lambda \odot \tilde{F} = (1+T)^\lambda \tilde{F}$. We now determine the quotient set

$$\mathbb{Z}_p[\![T]\!] / \sim_{\mathbb{Z}_p}$$

of the equivalence relation. Later this is needed to prove Theorem B.

Definition 53. Let

$$Q \subseteq \mathbb{Z}_{\geq 0} \times \big(\mathbb{Z}_p - \{0\}\big) \times \mathbb{Z}_{\geq 0} \times \mathbb{Z}_p[\![T]\!]$$

be the subset of elements $(m, a, r, P(T))$ which satisfy

$$0 \leq r \leq v_p(a).$$

We now prove the existence of an isomorphism

$$\mathbb{Z}_p[\![T]\!] / \sim_{\mathbb{Z}_p} \xrightarrow{\sim} \{0\} \cup Q.$$

We start with a trivial observation:

$$[0]_\sim = \{0\}.$$

Further we need the following

Lemma 54. *Let*

$$F(T) = a + bT + T^2 P(T^2)$$

an element of $\mathbb{Z}_p[\![T]\!]$ with $a \neq 0$.

i) There exists an unique element $r_F \in \{0, 1, \ldots, p^{v_p(a)} - 1\}$ such that

$$r_F \equiv b \mod a\mathbb{Z}_p.$$

ii) There exists an unique element $P_F(T) \in \mathbb{Z}_p[\![T]\!]$ such that

$$F \sim_{\mathbb{Z}_p} a + r_F T + T^2 P_F(T).$$

iii) Assume $b \in \{0, 1, \ldots, p^{v_p(a)} - 1\}$. Then $r_F = b$ and $P_F = P$.

Proof. i) This is a immediate consequence of the following equation:

$$\dot{\bigcup}_{r=0}^{p^{v(a)}-1} \left(r + c\mathbb{Z}_p\right) = \dot{\bigcup}_{r=0}^{p^{v(a)}-1} \left(r + p^{v(a)}\mathbb{Z}_p\right) = \mathbb{Z}_p.$$

ii) We start with the proof of the existence of P_F:
Example 38 states that

$$(1 + T)^\lambda = 1 + \lambda T + \mathcal{O}(T^2)$$

for all $\lambda \in \mathbb{Z}_p$. Let $l \in \mathbb{Z}_p$ be the unique element such that $r_F = b + la$. Then

$$\begin{aligned} la \odot F(T) &= (1 + T)^{la} F(T) = (1 + laT + \mathcal{O}(T^2))(a + bT + \mathcal{O}(T^2)) \\ &= a + (la + b)T + \mathcal{O}(T^2) = a + r_F T + \mathcal{O}(T^2) \end{aligned}$$

Let $P_F(T)$ be the unique element in $\mathbb{Z}_p[\![T]\!]$ such that we can write

$$la \odot F(T) = a + r_F T + T^2 P_F(T).$$

Now we prove the uniqueness:
Let $P_F(T)$ and $\hat{P}_F(T)$ be two polynomials such that

$$\left(a + r_F T + T^2 \hat{P}_F(T)\right) \sim_{\mathbb{Z}_p} F \sim_{\mathbb{Z}_p} \left(a + r_F T + T^2 P_F(T)\right)$$

Then there exists an p-adic integer λ such that

$$\left(a + r_F T + T^2 \hat{P}_F(T)\right) = (1 + T)^\lambda \left(a + r_F T + T^2 P_F(T)\right).$$

This imply

$$\begin{aligned} (a + r_F + \mathcal{O}(T^2)) &= (1 + \lambda T + \mathcal{O}(T^2))(a + r_F + \mathcal{O}(T^2)) \\ &= a + (r_F + \lambda a)T + \mathcal{O}(T^2) \end{aligned}$$

and since $a \neq 0$ this imply $\lambda = 0$. Therefore $P_F = \hat{P}_F$.

iii) This is obvious.

□

Regard that for every $F \in \mathbb{Z}_p[\![T]\!] - \{0\}$ there exists an unique non-negative integer m such that

$$F(T) = T^m(a + bT + \mathcal{O}(T^2))$$

with $a \neq 0$.

Corollary 55. *The map*

$$\phi : \Big(\mathbb{Z}_p[\![T]\!] - \{0\}\Big)/\sim_{\mathbb{Z}_p} \xrightarrow{\sim} Q$$

$$[F(T) = T^m(a + bT + \mathcal{O}(T^2))]_\sim \mapsto (m, a, r_F, P_F)$$

is a well-defined isomorphism with inverse isomorphism given by

$$Q \to \Big(\mathbb{Z}_p[\![T]\!] - \{0\}\Big)/\sim_{\mathbb{Z}_p}$$

$$(m, a, r, P(T)) \to [T^m(a + rT + T^2P(T))]_\sim.$$

In the later parts we need the following

Proposition 56. *i) The set*

$$1 + T\mathbb{Z}_p[\![T]\!]$$

is a $\mathbb{Z}_p$-invariant subset.

ii) There exists a bijection

$$(1 + T\mathbb{Z}_p[\![T]\!])/\sim_{\mathbb{Z}_p} \xrightarrow{\sim} \mathbb{Z}_p[\![T]\!].$$

Proof. i) This is trivial since $(1+T)^\lambda = (1 + \mathcal{O}(T))$.

ii) We show that the image of the injective map

$$\phi|_{(1+T\mathbb{Z}_p[\![T]\!])/\sim_{\mathbb{Z}_p}}$$

equals

$$\hat{Q} := \{0\} \times \{1\} \times \{0\} \times \mathbb{Z}_p[\![T]\!] \cong \mathbb{Z}_p[\![T]\!].$$

Let $F = 1 + bT + \mathcal{O}(T^2) \in 1 + T\mathbb{Z}_p[\![T]\!]$. Then we have $b \equiv 0 \mod 1\mathbb{Z}_p$, i.e. $r_F = 0$. Therefore $\phi([F]_\sim) = (0, 1, 0, P_F(T)) \in \hat{Q}$. If $P(T) \in \mathbb{Z}_p[\![T]\!]$ then

$$\phi([1 + T^2P(T)]_\sim) = (0, 1, 0, P(T)),$$

which imply the demanded.

□

The Amice transform of a measure

Let $\mu \in M(\mathbb{Z}_p, \mathbb{Z}_p)$. The Amice transform of μ is the map

$$\mathcal{F}_\mu : 1 + p\mathbb{Z}_p \to \mathbb{Z}_p$$

with

$$a \mapsto \int_{\mathbb{Z}_p} a^x d\mu(x).$$

Proposition 57. *If $a - 1 \in p\mathbb{Z}_p$ we have*

$$\mathcal{F}_\mu(a) = \int_{\mathbb{Z}_p} a^x d\mu(x) = F_\mu(a-1)$$

where

$$F_\mu = \sum_{n \geq 0} b_n(\mu)T^n \in \mathbb{Z}_p[\![T]\!]$$

is the power series corresponding to μ.

Proof. Let $b = a - 1$. In Example 38 we already showed that

$$(1+b)^x = \sum_{n\geq 0} \binom{x}{n} b^n$$

for all $x \in \mathbb{Z}_p$, which implies

$$\int_{\mathbb{Z}_p} (1+b)^x d\mu(x) = \int_{\mathbb{Z}_p} \sum_{n\geq 0} \binom{x}{n} b^n d\mu(x)$$

$$= \sum_{n\geq 0} \left(\int_{\mathbb{Z}_p} \binom{x}{n} d\mu(x) \right) b^n = \sum_{n\geq 0} b_n(\mu) b^n = F_\mu(b).$$

□

3.3 Measures on $\mathbb{Z}_p^\times/\{\pm 1\}$ and on $\Delta \times \mathbb{Z}_p$

In the rest of the section we use the notation

$$G := \mathbb{Z}_p^\times/\{\pm 1\}.$$

We start with the following

Lemma 58. *The map*

$$G \times M(G, \mathbb{Z}_p) \to M(G, \mathbb{Z}_p)$$
$$(\bar{\lambda}, \mu) \mapsto \bar{\lambda} \odot \mu$$

where $\bar{\lambda} \odot \mu$ is defined by

$$\int_G f d(\bar{\lambda} \odot \mu) = \int_G f(\bar{\lambda}\bar{x}) d\mu(\bar{x})$$

is a group action.

Proof. The map

$$\bar{\lambda} \odot \mu : \mathrm{cts}(G, \mathbb{Z}_p) \to \mathrm{cts}(G, \mathbb{Z}_p) \xrightarrow{\mu} \mathbb{Z}_p$$
$$f \mapsto f \circ (\cdot \bar{\lambda}) \mapsto \int_G f(\bar{\lambda}\bar{x}) d\mu(\bar{x})$$

is obviously $\mathbb{Z}_p$-linear. Since $(\cdot\bar{\lambda})$ and μ are continuous we have that $\bar{\lambda} \odot \mu$ is a measure. □

In this work we give several descriptions of $M(G, \mathbb{Z}_p)$. One of them in terms of sequences in $\mathbb{Q}_p$, one by using the Theory of measures on $\mathbb{Z}_p$.

Measures on $\mathbb{Z}_p^\times/\{\pm 1\}$ and sequences in $\mathbb{Q}_p$

There is an easy example of a continuous function $G \to \mathbb{Z}_p$.

Example 59. Assume k is an non-negative even integer. The assignment

$$\bar{x} \mapsto x^k$$

is a well-defined function $G \to \mathbb{Z}_p$, because $x^k = (-x)^k$. If a series $(\bar{x}_n)$ converges to $\bar{x}$ in G it is easy to see, that $x_n^k \to x^k$ in $\mathbb{Z}_p$. Therefore the function is continuous.

We use the $\prod^*$-notation described on page 7. An important observation is that there is a map

$$s : M(G, \mathbb{Z}_p) \to \prod_{\substack{k\geq 4 \\ k \text{ even}}} \mathbb{Q}_p = \prod_{k\geq 4}^{*} \mathbb{Q}_p$$

mapping a measure μ to the even sequence $(z_k)^*_{k\geq 4}$ defined by

$$z_k = \int_G x^k d\mu(\bar{x})$$

for even $k \geq 4$. We have the following obvious

Lemma 60. *The map*

$$s : M(G, \mathbb{Z}_p) \to \prod_{k\geq 4}^{*} \mathbb{Q}_p$$

is a $\mathbb{Z}_p$-module homomorphism. Therefore $\operatorname{im}(s)$ *is a $\mathbb{Z}_p$-submodule.*

Proof. Let $\mu, \nu \in M(G, \mathbb{Z}_p)$ and $\lambda \in \mathbb{Z}_2$. Then

$$s(\mu + \nu)_k = \int_G x^k d(\mu + \nu)(\bar{x}) = \int_G x^k d\mu(\bar{x}) + \int_G x^k d\nu(\bar{x}) = s(\mu)_k + s(\nu)_k$$

$$s(\lambda\mu)_k = \int_G x^k d(\lambda\mu)(\bar{x}) = \int_G \lambda x^k d(\mu)(\bar{x}) = \lambda s(\mu)_k$$

for even k. $\square$

Later the map s will become very important. We will see that s is injective and why the following definition deserve its name.

Definition 61. We say that a sequence

$$(z_k)^*_{k\geq 4} \in \prod_{k\geq 4}^{*} \mathbb{Q}_p$$

satisfies the generalized Kummer congruences if (z_k) is an element in the image of the $\mathbb{Z}_p$-module homomorphism

$$s : M(G, \mathbb{Z}) \to \prod_{k\geq 4}^{*} \mathbb{Q}_p.$$

We denote the $\mathbb{Z}_p$-module of sequences which satisfies the generalized Kummer congruences with **KC**.

Next we prove that **KC** is a G-set and the map $s : M(G, \mathbb{Z}) \to \mathbf{KC}$ is G-equivariant.

Lemma 62. *i) The map*

$$G \times \mathbf{KC} \to \mathbf{KC}$$

$$(\bar{\lambda}, (z_k)^*_{k\geq 4}) \mapsto \bar{\lambda} \odot (z_k)^*_{k\geq 4} := (\lambda^k z_k)^*_{k\geq 4}$$

is a well-defined group action.

ii) The map $s : M(G,\mathbb{Z}) \to \mathbf{KC}$ is G-equivariant.

Proof. Let $(z_k) \in \mathbf{KC}$. Remember that $\lambda^k z_k = (-\lambda)^k z_k$ for all even k. Then there exists a measure $\mu \in M(G,\mathbb{Z})$ such that $(z_k) = s(\mu)$ and this implies

$$z_k = \int_G x^k d\mu(\bar{x})$$

for all even k. Thus

$$\lambda^k z_k = \int_G \lambda^k x^k d\mu(\bar{x}) = \int_G x^k d(\bar{\lambda} \odot \mu)(\bar{x})$$

and therefore

$$(\lambda^k z_k)^*_{k\geq 4} = s(\bar{\lambda} \odot \mu).$$

Therefore $\bar{\lambda} \odot (z_k)^*_{k\geq 4} := (\lambda^k z_k)^*_{k\geq 4}$ is an element of $\mathbf{KC}$ and the group action is well-defined. It is obvious that $\bar{1} \odot (z_k)^*_{k\geq 4} = (z_k)^*_{k\geq 4}$ and that for $\bar{\kappa}, \bar{\lambda} \in G$ we have

$$\bar{\kappa} \odot (\bar{\lambda} \odot (z_k)^*_{k\geq 4}) = (\bar{\kappa}\bar{\lambda}) \odot (z_k)^*_{k\geq 4}.$$

For the equivariance of s: We have

$$s(\bar{\lambda} \odot \mu) = (\lambda^k z_k)^*_{k\geq 4} = \bar{\lambda} \odot (z_k)^*_{k\geq 4} = \bar{\lambda} \odot s(\mu).$$

□

Measures on $\Delta \times \mathbb{Z}_p$

The next goal is to describe an isomorphism of $\mathbb{Z}_p$-modules

$$M(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p) \xrightarrow{\sim} \bigoplus_{\theta \in \widehat{\Delta}} M(\mathbb{Z}_p, \mathbb{Z}_p).$$

Remember that a (Dirichlet) character of a finite abelian group H is a homomorphism $H \to \mathbb{C}^\times$. We use the notation $\widehat{H} := \hom_{group}(H, \mathbb{C}^\times)$ for the character group of H. The Teichmüller character ω described in Section 1 (see page 12) gives an unique element in $\widehat{(\mathbb{Z}/q\mathbb{Z})^\times}$ which makes the diagram

$$\begin{tikzcd} \mathbb{Z}_p^\times \arrow[r, "\omega"] \arrow[d, "\omega\circ\sigma"'] & \mu_{\tilde{q}} \subseteq \mathbb{C}^\times \\ (\mathbb{Z}/q\mathbb{Z})^\times \arrow[ur, dotted] & \end{tikzcd} \tag{63}$$

commutative. We denote this morphism $(\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$ also with ω and call it Teichmüller character. Later we need the following

Lemma 64. *Let H be a finite abelian group.*

i) H is non-canonically isomorphic to $\widehat{H}$.

ii) The Teichmüller character ω generates $\widehat{(\mathbb{Z}/q\mathbb{Z})^\times}$.

ii) The character ω^2 generates $\widehat{(\mathbb{Z}/q\mathbb{Z})^\times/\{\pm 1\}}$.

Proof. Part i) and Part ii) are known facts. Since the diagram

$$\begin{tikzcd}
(\mathbb{Z}/q\mathbb{Z})^\times \arrow[r, "\omega^2"] \arrow[d] & \mu_{\tilde{q}} \subseteq \mathbb{C}^\times \\
(\mathbb{Z}/q\mathbb{Z})^\times/\{\pm 1\} \arrow[ur, "\omega^2"] &
\end{tikzcd}$$

commutes, we know that the order of ω^2 equals

$$|\widehat{(\mathbb{Z}/q\mathbb{Z})^\times}|/2 = |\widehat{(\mathbb{Z}/q\mathbb{Z})^\times/\{\pm 1\}}|.$$

$\square$

The group Δ is finite and of order $(p-1)/2$. We use the notation $\widehat{\Delta} := \hom_{group}(\Delta, \mathbb{C}^\times)$ for the character group of Δ. For the description of $M(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p)$ we need the following

Lemma 65. *i) Every element $h \in \mathrm{cts}(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p)$ can be uniquely written as*

$$h(g, x) = \sum_{\theta \in \widehat{\Delta}} \theta(g) f_\theta(x)$$

for continuous functions $f_\theta \in \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p)$.

ii) The $\mathbb{Z}_p$-linear map

$$\mathrm{cts}(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p) \to \bigoplus_{\theta \in \widehat{\Delta}} \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p)$$

$$h(g, x) = \sum_{\theta \in \widehat{\Delta}} \theta(g) f_\theta(x) \mapsto (f_\theta)_{\theta \in \widehat{\Delta}}$$

is a topological isomorphism. The assignment, which maps a tupel $(f_\theta)_{\theta \in \widehat{\Delta}} \in \bigoplus \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p)$ to the continuous function

$$(g, x) \mapsto \sum_{\theta \in \widehat{\Delta}} \theta(g) f_\theta(x)$$

is obviously the inverse isomorphism.

Proof. Let $\gamma \in \widehat{\Delta}$. The element δ_γ in the group ring $\mathbb{Z}_p[\widehat{\Delta}]$ is defined by

$$\delta_\gamma(g) = \begin{cases} 1, & \text{if } g = \gamma \\ 0, & \text{else.} \end{cases}$$

We can write

$$h(g, x) = \sum_{\gamma \in \Delta} \delta_\gamma(g) h(\gamma, x).$$

Since $|\Delta|$ is prime to p it is invertible in $\mathbb{Z}_p$. In [S, Chapter 2] it is shown that

$$\sum_{\theta \in \widehat{\Delta}} \theta(g) = \begin{cases} |\Delta|, & \text{if } g = 1 \\ 0, & \text{else} \end{cases}$$

which implies

$$\delta_1(g) = \frac{1}{|\Delta|} \sum_{\theta \in \widehat{\Delta}} \theta(g) \in \mathbb{Z}_p[\widehat{\Delta}].$$

Translation with γ yields

$$\delta_\gamma(g) = \delta_1(g\gamma^{-1}) = \frac{1}{|\Delta|} \sum_{\theta \in \widehat{\Delta}} \theta(g)\theta(\gamma^{-1}) = \sum_{\theta \in \widehat{\Delta}} c_{\theta,\gamma}\theta(g)$$

for $c_{\theta,\gamma} := \frac{1}{|\Delta|}\theta(\gamma^{-1})$. The function $f_\theta : \mathbb{Z}_p \to \mathbb{Z}_p$ defined by

$$f_\theta(x) = \sum_{\gamma \in \Delta} c_{\theta,\gamma} h(\gamma, x)$$

is obviously continuous. Together with the above we have

$$h(g,x) = \sum_{\gamma \in \Delta} \left(\sum_{\theta \in \widehat{\Delta}} c_{\theta,\gamma}\theta(g) \right) h(\gamma, x) = \sum_{\theta \in \widehat{\Delta}} \theta(g) \sum_{\gamma \in \Delta} c_{\theta,\gamma} h(\gamma, x) = \sum_{\theta \in \widehat{\Delta}} \theta(g) f_\theta(x).$$

This proves Part i).

Now let $(h_n)_{n \geq 0} \subseteq \mathrm{cts}(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p)$ be a sequence converging to h, i.e.

$$\max_{(g,x) \in \Delta \times \mathbb{Z}_p} |h_n(g,x) - h(g,x)|_p \longrightarrow 0$$

There are continuous functions $f_\theta, f_{\theta,n} \in M(\mathbb{Z}_p, \mathbb{Z}_p)$ such that

$$h_n(g,x) = \sum_{\theta \in \widehat{\Delta}} \theta(g) f_{\theta,n}(x)\ , \qquad h(g,x) = \sum_{\theta \in \widehat{\Delta}} \theta(g) f_\theta(x).$$

We now show that the sequence $(f_{\theta,n})_{\theta \in \widehat{\Delta}}$ converges to $(f_\theta)_{\theta \in \widehat{\Delta}}$. Let $\vartheta \in \widehat{\Delta}$. By definition of $f_{\vartheta,n}, f_\vartheta$ we have

$$\begin{aligned} \max_{x \in \mathbb{Z}_p} |f_{\vartheta,n}(x) - f_\vartheta(x)|_p &= \max_{x \in \mathbb{Z}_p} \left| \sum_{\gamma \in \Delta} c_{\vartheta,\gamma}(h_n(\gamma,x) - h(\gamma,x)) \right|_p \\ &\leq \sum_{\gamma \in \Delta} c_{\vartheta,\gamma} \max_{x \in \mathbb{Z}_p} |h_n(\gamma,x) - h(\gamma,x)|_p \,. \end{aligned}$$

Since

$$\max_{x \in \mathbb{Z}_p} |h_n(\gamma,x) - h(\gamma,x)|_p \leq \max_{(g,x) \in \Delta \times \mathbb{Z}_p} |h_n(g,x) - h(g,x)|_p \longrightarrow 0$$

the claim of Part ii) is true. □

Corollary 66. *i) There is an well-defined isomorphism of $\mathbb{Z}_p$-modules*

$$\beta = (\beta_\theta)_{\theta \in \widehat{\Delta}} : M(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p) \xrightarrow{\sim} \bigoplus_{\theta \in \widehat{\Delta}} M(\mathbb{Z}_p, \mathbb{Z}_p)$$

$$\mu \mapsto \beta\mu = (\beta_\theta \mu)_{\theta \in \widehat{\Delta}}.$$

where $\beta_\theta\mu \in M(\mathbb{Z}_p, \mathbb{Z}_p)$ is defined by

$$\int_{\mathbb{Z}_p} f(x) d(\beta_\theta\mu)(x) := \int_{\Delta\times\mathbb{Z}_p} \theta(g) f(x) d\mu(g,x)$$

for all $f \in \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p)$.

ii) The inverse isomorphism

$$\beta^{-1} : \bigoplus_{\theta\in\widehat{\Delta}} M(\mathbb{Z}_p, \mathbb{Z}_p) \xrightarrow{\sim} M(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p)$$

maps an element $(\nu_\theta)_{\theta\in\widehat{\Delta}}$ to a element $\beta^{-1}((\nu_\theta)_{\theta\in\widehat{\Delta}}) \in M(\Delta\times\mathbb{Z}_p, \mathbb{Z}_p)$ which is well-defined by the formula

$$\int_{\Delta\times\mathbb{Z}_p} h(g,x)\, d\beta^{-1}((\nu_\theta))(g,x) = \int_{\Delta\times\mathbb{Z}_p} \sum_{\theta\in\widehat{\Delta}} \theta(g) f_\theta(x)\, d\beta^{-1}((\nu_\theta))(g,x) = \sum_{\theta\in\widehat{\Delta}} \int_{\mathbb{Z}_p} f_\theta\, d\nu_\theta,$$

for all $h \in \mathrm{cts}(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p)$, where the $f_\theta \in \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p)$ are chosen such that $h(g,x) = \sum \theta(g) f_\theta(x)$.

Proof. It is obvious that β and β^{-1} a $\mathbb{Z}_p$-module homomorphism. We split the proof up in three steps.

1) We show that β and β^{-1} are well-defined.

2) We show that $\beta \circ \beta^{-1}$ is the identity.

3) We show that $\beta^{-1} \circ \beta$ is the identity.

For Step 1): The map

$$\begin{aligned} \varphi : \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p) &\to \mathrm{cts}(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p) \\ f &\mapsto ((g,x) \mapsto \theta(g) f(x) \end{aligned}$$

is obviously continuous. Thus

$$\beta_\theta\mu : \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p) \xrightarrow{\varphi} \mathrm{cts}(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p) \xrightarrow{\mu} \mathbb{Z}_p$$

is continuous and therefore a measure.

Let $(\nu_\theta)_{\theta\in\widehat{\Delta}} \in \bigoplus M(\mathbb{Z}_p, \mathbb{Z}_p)$. The map

$$\begin{aligned} \beta^{-1}((\nu_\theta)) : \mathrm{cts}(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p) &\to \mathbb{Z}_p \\ h = \sum_{\theta\in\widehat{\Delta}} \theta(g) f_\theta(x) &\mapsto \sum_{\theta\in\widehat{\Delta}} \nu_\theta(f_\theta) \end{aligned}$$

can be written as a composition

$$\begin{aligned} \nu : \mathrm{cts}(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p) \xrightarrow{\sim} \bigoplus_{\theta\in\widehat{\Delta}} \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p) &\xrightarrow{(\nu_\theta)} \bigoplus_{\theta\in\widehat{\Delta}} \mathbb{Z}_p \to \mathbb{Z}_p \\ h \mapsto (f_\theta) \mapsto (\nu_\theta(f_\theta)) &\mapsto \sum_{\theta\in\widehat{\Delta}} \nu_\theta(f_\theta) \end{aligned}$$

where the left hand map the continuous $\mathbb{Z}_p$-linear map described in Lemma 65 Part ii) and the right hand map is the summation, which is also continuous and $\mathbb{Z}_p$-linear. Since the middle map is continuous and $\mathbb{Z}_p$-linear this is also true for $\beta^{-1}((\nu_\theta))$.

For Step 2): Let $f \in \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p)$ and $(\nu_\theta)_{\theta\in\widehat{\Delta}} \in \bigoplus M(\mathbb{Z}_p, \mathbb{Z}_p)$. We have to show that $\beta_\theta(\beta^{-1}((\nu_\theta))) = \nu_\theta$ for all $\theta \in \widehat{\Delta}$. Using first Part i) and then Part ii) we get that

$$\int_{\mathbb{Z}_p} f d\beta_\theta(\beta^{-1}((\nu_\theta))) = \int_{\Delta\times\mathbb{Z}_p} \theta(g) f(x) d\beta^{-1}((\nu_\theta))(x, g) = \int_{\mathbb{Z}_p} f d\nu_\theta.$$

For Step 3): Let $h(g, x) = \sum \theta(g) f_\theta(x) \in \mathrm{cts}(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p)$ and $\mu \in M(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p)$. We have

$$\int_{\Delta\times\mathbb{Z}_p} h d\mu = \int_{\Delta\times\mathbb{Z}_p} \sum_{\theta\in\widehat{\Delta}} \theta(g) f_\theta(x) d\mu(g, x)$$

$$= \sum_{\theta\in\widehat{\Delta}} \int_{\Delta\times\mathbb{Z}_p} \theta(g) f_\theta(x) d\mu(g, x).$$

Using Part i) we get that this is equal to

$$\sum_{\theta\in\widehat{\Delta}} \int_{\mathbb{Z}_p} f_\theta(x) d(\beta_\theta\mu)(x)$$

Using Part ii) we get that this is equal to

$$\int_{\Delta\times\mathbb{Z}_p} \sum_{\theta\in\widehat{\Delta}} \theta(g) f_\theta(x) d\beta^{-1}((\beta_\theta\mu))(g, x) = \int_{\Delta\times\mathbb{Z}_p} h d\beta^{-1}(\beta(\mu)).$$

□

The equivariance of β

Remember that $M(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p)$ carries the structure of a $\mathbb{Z}_p$ -algebra. This endows

$$\bigoplus_{\theta\in\widehat{\Delta}} M(\mathbb{Z}_p, \mathbb{Z}_p)$$

canonically with a $\mathbb{Z}_p$-algebra structure. Therefore the $\mathbb{Z}_p$-module isomorphism

$$\beta : M(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p) \xrightarrow{\sim} \bigoplus_{\theta\in\widehat{\Delta}} M(\mathbb{Z}_p, \mathbb{Z}_p)$$

induces a $\mathbb{Z}_p$-algebra structure on $M(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p)$.

Lemma 67. *The map*

$$(\Delta \times \mathbb{Z}_p) \times M(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p) \to M(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p)$$

$$((\xi, \lambda), \mu) \mapsto (\xi, \lambda) \odot \mu$$

where $(\xi, \lambda) \odot \mu$ *is defined by*

$$\int_{\Delta\times\mathbb{Z}_p} f(g,x)d\Big((\xi,\lambda)\odot\mu\Big)(g,x) = \int_{\Delta\times\mathbb{Z}_p} f(\xi g, x+\lambda)d\mu(g,x)$$

is a well-defined group action.

Proof. The map

$$(\xi,\lambda)\odot\mu : \mathrm{cts}(\Delta\times\mathbb{Z}_p,\mathbb{Z}_p) \to \mathrm{cts}(\Delta\times\mathbb{Z}_p,\mathbb{Z}_p) \xrightarrow{\mu} \mathbb{Z}_p$$
$$f \mapsto f\circ(\cdot\xi,+\lambda) \mapsto \int_{\Delta\times\mathbb{Z}_p} f(\xi g, x+\lambda)d\mu(g,x)$$

is obviously $\mathbb{Z}_p$-linear. Since $(\cdot\xi,+\lambda)$ and μ are continuous we have that $(\xi,\lambda)\odot\mu$ is a measure. □

Remember that there is a $\mathbb{Z}_p$ action on $M(\mathbb{Z}_p,\mathbb{Z}_p)$ such that

$$\int f d\lambda\odot\mu = \int f(\lambda+x)d\lambda$$

for all $\lambda\in\mathbb{Z}_2$, $\mu\in M(\mathbb{Z}_p,\mathbb{Z}_p)$ and continuous functions f. (See Lemma 51)

Lemma 68. *The map*

$$(\Delta\times\mathbb{Z}_p)\times\bigoplus_{\theta\in\widehat{\Delta}} M(\mathbb{Z}_p,\mathbb{Z}_p) \to \bigoplus_{\theta\in\widehat{\Delta}} M(\mathbb{Z}_p,\mathbb{Z}_p)$$

$$((\xi,\lambda),(\mu_\theta)_{\theta\in\widehat{\Delta}}) \mapsto (\xi,\lambda)\odot(\mu_\theta)_{\theta\in\widehat{\Delta}} := \Big(\theta(\xi)\cdot(\lambda\odot\mu_\theta)\Big)_{\theta\in\widehat{\Delta}}$$

is a well-defined group action.

Proof. This is obvious since we already proved that $(\lambda,\mu_\theta)\to\lambda\odot\mu_\theta$ is a group action (See Lemma 51) and θ is a multiplicative group homomorphism. □

In Proposition 47 and Lemma 52 we proved the existence of an isomorphism of $\mathbb{Z}_p$-algebras

$$F_\bullet : M(\mathbb{Z}_p,\mathbb{Z}_p) \xrightarrow{\sim} \mathbb{Z}_p[\![T]\!]$$

which is $\mathbb{Z}_p$-equivariant Remember that the $\mathbb{Z}_p$ action on $\mathbb{Z}_p[\![T]\!]$ is given by

$$\lambda\odot F(T) = (1+T)^\lambda F(T)$$

for all $\lambda\in\mathbb{Z}_2$ and $F(T)\in\mathbb{Z}_p[\![T]\!]$.

Lemma 69. *The map*

$$(\Delta\times\mathbb{Z}_p)\times\bigoplus_{\theta\in\widehat{\Delta}}\mathbb{Z}_p[\![T]\!] \to \bigoplus_{\theta\in\widehat{\Delta}}\mathbb{Z}_p[\![T]\!]$$

$$((\xi,\lambda),(F_\theta)_{\theta\in\widehat{\Delta}}) \mapsto (\xi,\lambda)\odot(F_\theta)_{\theta\in\widehat{\Delta}} := \Big(\theta(\xi)(\lambda\odot F_\theta)\Big)_{\theta\in\widehat{\Delta}}$$

is a well-defined group action.

Proof. This is obvious since we already proved that $(\lambda,F_\theta(T))\to\lambda\odot F_\theta$ is a group action (See Lemma 52) and θ is a multiplicative group homomorphism. □

Remember that we have an isomorphism of topological groups (see Corollary 11)

$$\alpha : G = \mathbb{Z}_p^\times/\{\pm 1\} \to \Delta \times \mathbb{Z}_p$$
$$\bar{x} \mapsto \left((\sigma \circ \omega)(x), \frac{\log_p \langle x \rangle}{\log_p(1+p)} \right).$$

This isomorphism endows the $\Delta \times \mathbb{Z}_p$-sets

$$M(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p) \quad \text{and} \quad \bigoplus_{\theta \in \widehat{\Delta}} M(\mathbb{Z}_p, \mathbb{Z}_p) \quad \text{and} \quad \bigoplus_{\theta \in \widehat{\Delta}} \mathbb{Z}_p[\![T]\!]$$

with a G-set structure by defining

$$g \odot x := \alpha(g) \odot x$$

for every $g \in G$ and every element x in one of the three sets. Finally we get

Proposition 70. *i) The isomorphism of $\mathbb{Z}_p$-algebras*

$$\beta = (\beta_\theta)_{\theta \in \widehat{\Delta}} : M(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p) \xrightarrow{\sim} \bigoplus_{\theta \in \widehat{\Delta}} M(\mathbb{Z}_p, \mathbb{Z}_p)$$

is G-equivariant.

ii) The isomorphism of $\mathbb{Z}_p$-algebras

$$\oplus_{\theta \in \widehat{\Delta}} F_\bullet : \bigoplus_{\theta \in \widehat{\Delta}} M(\mathbb{Z}_p, \mathbb{Z}_p) \xrightarrow{\sim} \bigoplus_{\theta \in \widehat{\Delta}} \mathbb{Z}_p[\![T]\!]$$

is G-equivariant.

Proof. It is enough to show that the morphisms in i) and ii) are $\Delta \times \mathbb{Z}_p$-equivariant. Let $r := (\xi, \lambda) \in \Delta \times \mathbb{Z}_p$. Let $f \in \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p)$. Let ν_θ be the θ-component of $r \odot \beta(\mu)$ and $\tilde{\nu}_\theta$ be the θ-component of $\beta(r \odot \mu)$. Corollary 66 together with Lemma 69 gives us

$$\int_{\mathbb{Z}_p} f(x) d\nu_\theta(x) = \int_{\mathbb{Z}_p} \theta(\xi) f(x) d(\lambda \odot \beta_\theta \mu)(x) = \int_{\mathbb{Z}_p} \theta(\xi) f(x+\lambda) d\beta_\theta \mu(x)$$
$$= \int_{\Delta \times \mathbb{Z}_p} \theta(g)\theta(\xi) f(x+\lambda) d\mu(g,x) = \int_{\Delta \times \mathbb{Z}_p} \theta(\xi g) f(\lambda + x) d\mu(g,x)$$

and

$$\int_{\mathbb{Z}_p} f(x) d\tilde{\nu}_\theta(x) = \int_{\mathbb{Z}_p} f(x) d\big(\beta_\theta((\xi,\lambda) \odot \mu)\big)(x)$$
$$= \int_{\Delta \times \mathbb{Z}_p} \theta(g) f(x) d\big((\xi,\lambda) \odot \mu\big)(x) = \int_{\Delta \times \mathbb{Z}_p} \theta(\xi g) f(\lambda + x) d\mu(g,x).$$

This proves Part i).

Let $(\mu_\theta) \in \bigoplus_{\theta \in \widehat{\Delta}} M(\mathbb{Z}_p, \mathbb{Z}_p)$. Then

$$(\oplus_{\theta \in \widehat{\Delta}} F_\bullet)(r \odot (\mu_\theta)_{\theta \in \widehat{\Delta}}) = (\oplus_{\theta \in \widehat{\Delta}} F_\bullet)\Big((\theta(\xi)(\lambda \odot \mu_\theta))_{\theta \in \widehat{\Delta}} \Big).$$

Since $F_\bullet$ is $\mathbb{Z}_p$-equivariant and $\mathbb{Z}_p$-linear we have that the right hand side of this equation is

$$\Big(\theta(\xi) F_{\lambda \odot \mu_\theta}\Big)_{\theta \in \widehat{\Delta}} = \Big(\theta(\xi)(\lambda \odot F_{\mu_\theta})\Big)_{\theta \in \widehat{\Delta}} = r \odot (F_{\mu_\theta})_{\theta \in \widehat{\Delta}}.$$

This proves Part ii). $\square$

3.4 Power series and Measures on $\mathbb{Z}_p^\times/\{\pm 1\}$

The isomorphism of topological groups

$$\alpha = (\gamma, l) : G = \mathbb{Z}_p^\times/\{\pm 1\} \to \Delta \times \mathbb{Z}_p$$

$$\bar{x} \mapsto \left((\sigma \circ \omega)(x), \frac{\log_p \langle x \rangle}{\log_p (1+p)} \right)$$

described in Corollary 11 induces an isomorphism of $\mathbb{Z}_p$-modules

$$a_* : M(G, \mathbb{Z}_p) \xrightarrow{\sim} M(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p)$$

such that

$$\int_{\Delta \times \mathbb{Z}_p} f(g,x) d\alpha_* \mu(g,x) = \int_G f(\gamma(\bar{t}), l(\bar{t})) d\mu(\bar{t})$$

for all continuous functions f on $\Delta \times \mathbb{Z}_p$ and all measures $\mu \in M(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p)$ (See Lemma 31). The set $M(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p)$ carries the structure of a $\mathbb{Z}_p$-algebra, therefore α induces a $\mathbb{Z}_p$-algebra structure on $M(G, \mathbb{Z}_p)$. Further we have

Lemma 71. *The isomorphism of $\mathbb{Z}_p$-algebras*

$$\alpha_* : M(G, \mathbb{Z}_p) \xrightarrow{\sim} M(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p)$$

is G-equivariant.

Proof. Let $\bar{g} \in G$ and $(\xi, \lambda) := \alpha_*(\bar{g}) \in \Delta \times \mathbb{Z}_p$. Let f be a continuous function on $\Delta \times \mathbb{Z}_p$ and $\mu \in M(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p)$. Then

$$\alpha_*(g \odot \mu)(f) = \int_G f(\gamma(\bar{t}), l(\bar{t})) d(\bar{g} \odot \mu)(\bar{t}) = \int_G f(\gamma(\bar{g}\bar{t}), l(\bar{g}\bar{t})) d\mu(\bar{t}).$$

Remember that by definition we have $\bar{g} \odot \alpha_*(\mu) = \alpha(\bar{g}) \odot \alpha_*(\mu) = (\xi, \lambda) \odot \alpha_*(\mu)$ and therefore

$$\begin{aligned}
\big((\xi, \lambda) \odot \alpha_*(\mu)\big)(f) &= \int_{\Delta \times \mathbb{Z}_p} f(\gamma, x) d\big((\xi, \lambda) \odot \alpha_*(\mu)\big)(\gamma, x) \\
&= \int_{\Delta \times \mathbb{Z}_p} f(\xi\gamma, \lambda + x) d\big(\alpha_*(\mu)\big)(\gamma, x) \\
&= \int_G f(\xi\gamma(\bar{t}), \lambda + l(\bar{t})) d\mu(\bar{t}).
\end{aligned}$$

Since $\xi\gamma(\bar{t}) = \gamma(\bar{g})\gamma(\bar{t}) = \gamma(\bar{g}\bar{t})$ and $\lambda + l(\bar{t}) = l(\bar{g}) + l(\bar{t}) = l(\bar{g}\bar{t})$ for all $\bar{t} \in G$ the claim of the Lemma is proved. $\square$

Now we put the pieces together. Proposition 70 together with Lemma 71 gives us an isomorphism of $\mathbb{Z}_p$-algebras

$$\psi_1 : M(G, \mathbb{Z}_p) \xrightarrow{\alpha_*} M(\Delta \times \mathbb{Z}_p, \mathbb{Z}_p) \xrightarrow{\beta} \bigoplus_{\theta \in \widehat{\Delta}} M(\mathbb{Z}_p, \mathbb{Z}_p) \xrightarrow{\oplus F_\bullet} \bigoplus_{\theta \in \widehat{\Delta}} \mathbb{Z}_p[\![T]\!]$$

which is G-equivariant.

Since ω^2 is a generator $\widehat{\Delta}$ there is a canonical isomorphism of $\mathbb{Z}_p$-algebras

$$\bigoplus_{r\in\mathbb{Z}/(|\Delta|)} \mathbb{Z}_p[\![T]\!] \xrightarrow{\sim} \bigoplus_{\theta\in\widehat{\Delta}} \mathbb{Z}_p[\![T]\!]$$

$$(F_r) \mapsto (F_{\omega^{2r}})$$

or equivalently

$$\psi_2 : \bigoplus_{\substack{r\in\mathbb{Z}/(2|\Delta|)\\ r \text{ even}}} \mathbb{Z}_p[\![T]\!] \xrightarrow{\sim} \bigoplus_{\theta\in\widehat{\Delta}} \mathbb{Z}_p[\![T]\!]$$

$$(F_r) \mapsto (F_{\omega^r})$$

Then ψ transports the G-set structure of the left-hand side to the right hand side, i.e.

$$\bigoplus_{\substack{r\in\mathbb{Z}/(2|\Delta|)\\ r \text{ even}}} \mathbb{Z}_p[\![T]\!]$$

carries a G-action defined by

$$g \odot (F_r) = \psi^{-1}(g \odot (F_{\omega^r}))$$

for all $g \in G$ and tuples (F_r).

Remember we use the notation

$$\tilde{q} := \begin{cases} p-1 & \text{if } p \text{ odd} \\ 2 & \text{if } p = 2 \end{cases}$$

and the $\prod^*$-notation described on page 7. Regard that $\frac{1}{2}\tilde{q} = |\widehat{\Delta}| = |\Delta|$ and therefore

$$\bigoplus_{\substack{r\in\mathbb{Z}/(2|\Delta|)\\ r \text{ even}}} \mathbb{Z}_p[\![T]\!] =: \bigoplus_{r\in\mathbb{Z}/\tilde{q}}^{*} \mathbb{Z}_p[\![T]\!].$$

Remember that Lemma 62 states that the $\mathbb{Z}_p$-module homomorphism

$$s : M(G,\mathbb{Z}_p) \to \mathbf{KC} \subseteq \prod_{k\geq 4}^{*} \mathbb{Q}_p$$

is G-equivariant. We get

Proposition 72. *The G-equivariant isomorphism of $\mathbb{Z}_p$-modules*

$$\Phi_1 : M(G,\mathbb{Z}_p) \xrightarrow{\psi_1} \bigoplus_{\theta\in\widehat{\Delta}} \mathbb{Z}_p[\![T]\!] \xrightarrow{\psi_2^{-1}} \bigoplus_{r\in\mathbb{Z}/\tilde{q}}^{*} \mathbb{Z}_p[\![T]\!].$$

maps an element $\mu \in M(G,\mathbb{Z}_p)$ to the element

$$\left(\sum_{n\geq 0} a_{r,n} T^n\right)^{*}_{r\in\mathbb{Z}/\tilde{q}}$$

where

$$a_{r,n} = \int_G \omega^r(\bar{t}) \binom{(\log_p(1+q))^{-1}\log_p\langle t\rangle}{n}\, d\mu(\bar{t})$$

for all $n \geq 0$. In particular we have

$$a_{0,0} = \int_G 1\, d\mu.$$

Proof. We have

$$\Phi_1(\mu) = \Big(\psi_2^{-1} \circ (\oplus_\theta F_\bullet) \circ \beta \circ \alpha_*\Big)(\mu)$$

and because

$$\big(\oplus_\theta F_\bullet\big)\big((\beta_\theta \alpha_* \mu)_\theta\big) = \Big(F_\bullet(\beta_\theta \alpha_* \mu)\Big)_\theta$$

we have

$$\Phi_1(\mu) = \Big(F_\bullet(\beta_{\omega^r}\alpha_*\mu)\Big)^*_{r\in\mathbb{Z}/\tilde{q}}.$$

Diagram 63 tells us that we have a commutative diagram

$$\begin{tikzcd} G = \mathbb{Z}_p^\times/\{\pm 1\} \arrow[r, "\omega^r"] \arrow[d, "\gamma"'] & \mu_{\tilde{q}} \subseteq \mathbb{C}^\times \\ \Delta = (\mathbb{Z}/q\mathbb{Z})^\times/\{\pm 1\} \arrow[ur, "\omega^r"'] & \end{tikzcd}$$

for even k. Therefore $\omega^r(\gamma(\bar{t})) = \omega^r(\bar{t})$ for all $\bar{t} \in G$ and even r. We have

$$F_\bullet(\beta_{\omega^r}\alpha_*\mu) = \sum_{n\geq 0} b_n(\beta_{\omega^r}\alpha_*\mu)T^n$$

where (see Lemma 47 and Corollary 66)

$$\begin{aligned} b_n(\beta_{\omega^r}\alpha_*\mu) &= \int_{\mathbb{Z}_p} \binom{x}{n}\, d\big(\beta_{\omega^r}\alpha_*\mu\big)(x) = \int_{\Delta\times\mathbb{Z}_p} \omega^r(g)\binom{x}{n}\, d\big(\alpha_*\mu\big)(g,x) \\ &= \int_G \omega^r(\bar{t}) \binom{(\log_p(1+q))^{-1}\log_p\langle t\rangle}{n}\, d\mu(\bar{t}). \end{aligned}$$

$\square$

Now we state and prove the main Theorem of this section.

Theorem 73. *i) The G-equivariant homomorphism of $\mathbb{Z}_p$-modules* [2]

$$\Gamma : \bigoplus_{r\in\mathbb{Z}/\tilde{q}}^{*} \mathbb{Z}_p[\![T]\!] \xrightarrow{\Phi_1^{-1}} M(G,\mathbb{Z}_p) \xrightarrow{s} \mathbf{KC} \subseteq \prod_{k\geq 4}^{*} \mathbb{Q}_p$$

maps an element

$$(F_r)^*_{r\in\mathbb{Z}/\tilde{q}} \in \bigoplus_{r\in\mathbb{Z}/\tilde{q}}^{*} \mathbb{Z}_p[\![T]\!]$$

to the sequence

$$\Big(F_k\big((1+q)^k - 1\big)\Big)^*_{k\geq 4}.$$

[2] Remember that this is exactly the map of Definition 22

ii) The homomorphism of $\mathbb{Z}_p$-modules

$$\Gamma : \bigoplus_{r\in\mathbb{Z}/\tilde{q}}^{*} \mathbb{Z}_p[\![T]\!] \longrightarrow \prod_{k\geq 4}^{*} \mathbb{Q}_p$$

is a homomorphism of $\mathbb{Z}_p$-algebras. Therefore the $\mathbb{Z}_p$-module $\mathbf{KC} = \mathrm{im}(\Gamma)$ *is a $\mathbb{Z}_p$-subalgebra.*

Proof. Let $(F_r), (H_r) \in \bigoplus^{*}_{r\in\mathbb{Z}/\tilde{q}} \mathbb{Z}_p[\![T]\!]$ and

$$\mu := (\psi_1^{-1} \circ \psi_2)\Big((F_r)^{*}_{r\in\mathbb{Z}/\tilde{q}}\Big).$$

First we have to show that

$$s(\mu) = \int_G \bar{t}^k d\mu(\bar{t}) = F_k((1+q)^k - 1)$$

for all even $k \geq 4$. Then Proposition 57 imply that

$$F_k((1+q)^k - 1) = F_{\omega^k}((1+q)^k - 1) = \int_{\mathbb{Z}_p} (1+q)^{kx} d\mu_{\omega^k}(x)$$

where $\mu_{\omega^k} := (F_\bullet)^{-1}(F_{\omega^k}) \in M(\mathbb{Z}_p, \mathbb{Z}_p)$. Since $\mu_{\omega^k} = \beta_{\omega^k}(\alpha_*(\mu))$ we get from Corollary 66 that

$$\begin{aligned}\int_{\mathbb{Z}_p} (1+q)^{kx} d\mu_{\omega^k}(x) &= \int_{\Delta\times\mathbb{Z}_p} \omega^k(g)(1+q)^{kx} d(\alpha_*\mu)(g,x) \\ &= \int_G \omega^k(\gamma(\bar{t}))(1+q)^{kl(\bar{t})} d\mu(\bar{t})\end{aligned}$$

with $\alpha(\bar{t}) = (\gamma(\bar{t}), l(\bar{t}))$ for all $\bar{t} \in G$. Diagram 63 tells us that we have a commutative diagram

$$\begin{tikzcd} G = \mathbb{Z}_p^\times/\{\pm 1\} \arrow[r, "\omega^k"] \arrow[d, "\gamma"'] & \mu_{\tilde{q}} \subseteq \mathbb{C}^\times \\ \Delta = (\mathbb{Z}/q\mathbb{Z})^\times/\{\pm 1\} \arrow[ur, "\omega^k"'] & \end{tikzcd}$$

for even k. Therefore $\omega^k(\gamma(\bar{t})) = \omega^k(\bar{t})$ for all $\bar{t} \in G$ and even $k \geq 4$. Further we have that

$$(1+q)^{kl(\bar{t})} = \exp\big(kl(\bar{t})\log_p(1+q)\big) = \exp\left(k\frac{\log_p\langle t\rangle}{\log_p(1+q)}\log_p(1+q)\right) = \langle t\rangle^k.$$

Remember that $\bar{t}^k = \omega^k(\bar{t})\langle t\rangle$ for all $\bar{t} \in G$ and even k (see page 12 - 13). Therefore we have that

$$\int_G \omega^k(\gamma(\bar{t}))(1+q)^{kl(\bar{t})} d\mu(\bar{t}) = \int_G \omega^k(\bar{t})\langle t\rangle d\mu(\bar{t}) = \int_G \bar{t}^k d\mu(\bar{t}).$$

This proves Part i). Part ii) is immediately implied by Part i) because

$$\begin{aligned}\Big(\Gamma\big((F_r H_r)\big)\Big)_k &= (F_k H_k)((1+q)^k - 1) \\ &= F_k((1+q)^k - 1) \cdot H_k((1+q)^k - 1) = (\Gamma\big((F_r)\big))_k \cdot (\Gamma\big((H_r)\big))_k .\end{aligned}$$

$\square$

Kummer congruences and p-local series I

Let $c \in \mathbb{Z}_p^\times$ be an element which projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$. In this and the next paragraph we give two additional descriptions of $M(G, \mathbb{Z}_p)$ in terms of zero sequences of p-adic integers. The intention to do this, is the hope that this descriptions will help to attack part ii) of Problem 23.

Let $r \in \mathbb{Z}/\tilde{q}$ with r even. Remember (Definition 24) that we have a $\mathbb{Z}_p$-module homomorphism

$$\Gamma_r : \mathbb{Z}_p[\![T]\!] \to \prod_{\substack{k \geq 4 \\ k \equiv r \bmod \tilde{q}}} \mathbb{Q}_p$$

$$F \mapsto \Big(F\big((1+q)^k - 1\big) \Big)_{\substack{k \geq 4 \\ k \equiv r \bmod \tilde{q}}}$$

and that $\Gamma = \bigoplus^*_{r \in \mathbb{Z}/\tilde{q}} \Gamma_r$. We use the injective map

$$\kappa_1 : \mathbb{Z}_p[\![T]\!] \hookrightarrow \mathrm{cts}(\mathbb{Z}_p, \mathbb{Z}_p) \xrightarrow{\sim} c_0(\mathbb{Z}_p)$$

$$F = \sum a_m T^m \mapsto \big(x \mapsto F(px)\big) \mapsto \left(\int_{\mathbb{Z}_p} F(px)\, d\varrho_n(x) \right)_{n \geq 0} = \left(\sum_{m \geq 0} a_m p^m \int_{\mathbb{Z}_p} x^m \, d\varrho_n(x) \right)_{n \geq 0} .$$

described on page 29. Remember (Proposition 40) that

$$\mathbf{X}_1 = \mathrm{im}(\kappa_1) = \left\{ (b_n)_{n \geq 0} \in c_0(\mathbb{Z}_p) \;\middle|\; \frac{b_n}{n!\, p^n} \in \mathbb{Z}_p \right\}.$$

Proposition 74. *For a non-negative integer k let $\hat{p}_k := p^{-1}\big((1+q)^k - 1\big)$. We have a commutative diagram of $\mathbb{Z}_p$-module homomorphisms*

$$\begin{tikzcd} & \mathbb{Z}_p[\![T]\!] \arrow[dl, "\sim"', "\kappa_1"] \arrow[dr, "\Gamma_r"] & \\ \mathbf{X}_1 \arrow[rr, "\hat{\Gamma}_{1,r}"'] & & \prod\limits_{\substack{k \geq 4 \\ k \equiv r \bmod \tilde{q}}} \mathbb{Q}_p \end{tikzcd}$$

where

$$\hat{\Gamma}_{1,r} : \mathbf{X}_1 \to \prod_{\substack{k \geq 4 \\ k \equiv r \bmod \tilde{q}}} \mathbb{Q}_p$$

is given by

$$(b_n)_{n \geq 0} \mapsto \left(\sum_{n=0}^{\hat{p}_k} b_n \binom{\hat{p}_k}{n} \right)_k = \Big(\big(\kappa_1^{-1}(b_n)_{n \geq 0}\big)\big((1+q)^k - 1\big) \Big)_k .$$

Proof. Let $(b_n)_{n \geq 0} \in \mathbf{X}_1$. Regard that

$$F(px) = \sum_{n \geq 0} b_n \binom{x}{n}$$

for all $x \in \mathbb{Z}_p$. Therefore

$$\Gamma_r(F) = \Big(F\Big(pp^{-1}\big((1+q)^k - 1\big)\Big)\Big)_{\substack{k\geq 4 \\ k\,\equiv\, r \bmod \tilde{q}}} = \left(\sum_{n\geq 0} b_n \binom{\hat{p}_k}{n}\right)_{\substack{k\geq 4 \\ k\,\equiv\, r \bmod \tilde{q}}} = \hat{\Gamma}_{1,r}((b_n)).$$

□

Corollary 75. *We have a commutative diagram of $\mathbb{Z}_p$-module homomorphisms*

$$\begin{tikzcd} M(G,\mathbb{Z}_p) \arrow[r, "\sim"] & \overset{*}{\bigoplus\limits_{r\in\mathbb{Z}/\tilde{q}}} \mathbb{Z}_p[\![T]\!] \arrow[rr, "\sim", "\oplus\kappa_1"'] \arrow[dr, "\Gamma"'] & & \overset{*}{\bigoplus\limits_{r\in\mathbb{Z}/\tilde{q}}} \mathbf{X}_1 \arrow[dl, "\hat{\Gamma}_1"] \\ & & \mathbf{KC} & \end{tikzcd}$$

where

$$\hat{\Gamma}_1 : \overset{*}{\bigoplus_{r\in\mathbb{Z}/\tilde{q}}} \mathbf{X}_1 \overset{\oplus\hat{\Gamma}_{1,r}}{\longrightarrow} \overset{*}{\bigoplus_{r\in\mathbb{Z}/\tilde{q}}} \left(\prod_{\substack{k\geq 4 \\ k\,\equiv\, r \bmod \tilde{q}}} \mathbb{Q}_p\right) \cong \overset{*}{\prod_{k\geq 4}} \mathbb{Q}_p.$$

The hope was, that the pre-image

$$\hat{\Gamma}_1^{-1}\left(\mathbf{ConB}_c\right)$$

is easier to find than

$$\Gamma^{-1}\left(\mathbf{ConB}_c\right)$$

since the components of $\hat{\Gamma}_{1,r}(F)$ are, other than the component of $\Gamma_r(F)$, finite sums. Unfortunately this was not successful. Nevertheless this new representation brings us additional information.

Lemma 76. *i) Let $r \in \mathbb{Z}/\tilde{q}$ with r even. Then*

$$\mathbf{Y} := \mathbf{X}_1 \cap c_0(\mathbb{Z}_{(p)}) \subseteq \hat{\Gamma}_{1,r}^{-1}\left(\prod_{\substack{k\geq 4 \\ k\,\equiv\, r \bmod \tilde{q}}} \mathbb{Z}_{(p)}\right).$$

ii) Assume

$$\kappa_1\left(\sum_{m\geq 0} a_m T^m\right) = (b_n)_{n\geq 0} \in \mathbf{X}_1.$$

Then $a_0 = b_0$.

Proof. i) Let $(b_n)_{n\geq 0} \in \mathbf{X}_1 \cap c_0(\mathbb{Z}_{(p)})$. Since $\hat{p}_k \in \mathbb{N}_0$ we have that

$$\hat{\Gamma}_{1,r}((b_n)_{n\geq 0}) = \left(\sum_{n=0}^{\hat{p}_k} b_n \binom{\hat{p}_k}{n}\right)_k$$

is obviously an element of

$$\prod_{\substack{k\geq 4\\ k\equiv r \bmod \tilde{q}}} \mathbb{Z}_{(p)}.$$

ii) We have

$$b_0=\sum_{m\geq 0} a_m \int_{\mathbb{Z}_p} x^m p^m d\varrho_0 = \sum_{m\geq 0} a_m (x^m|_{x=0}) = a_0.$$

□

Kummer congruences and p-local series II

Let $r\in \mathbb{Z}/\tilde{q}$ with r even. We know describe the second approach. Let $\gamma_r:\mathbb{Z}_p\to\mathbb{Z}_p$ be the map given by

$$x\mapsto (1+q)^{\tilde{q}x+u}-1.$$

where $u:=\min\{k\geq 4 \mid k\equiv r \mod \tilde{q}\}$. We now use the injective map

$$\kappa_{2,r}:\mathbb{Z}_p[\![T]\!]\to \mathrm{cts}(\mathbb{Z}_p,\mathbb{Z}_p)\xrightarrow{\sim} c_0(\mathbb{Z}_p)$$

$$\begin{aligned} F=\sum a_m T^m \mapsto \big(x\mapsto F(\gamma_r(x))\big) &\mapsto \left(\int_{\mathbb{Z}_p} F(\gamma_r(x))\, d\varrho_n(x)\right)_{n\geq 0} \\ &= \left(\sum_{m\geq 0} a_m \int_{\mathbb{Z}_p} \gamma_r^m(x)\, d\varrho_n(x)\right)_{n\geq 0}. \end{aligned}$$

described on page 30. Let $\mathbf{X}_{2,r}:=\mathrm{im}(\kappa_{2,r})$.

Remark 77. Remember that Corollary 45 states that

$$\int_{\mathbb{Z}_p} \gamma_r^m(x)\, d\varrho_n(x) = \int_{\mathbb{Z}_p} (1+q)^{ux}\gamma_0^n(x)\, d\varrho_m(x).$$

Let $\mu_F\in M(\mathbb{Z}_p,\mathbb{Z}_p)$ be the measure corresponding to F, i.e.

$$\int_{\mathbb{Z}_p} f\, d\mu_F(x) = \sum_{m\geq 0} a_m \int_{\mathbb{Z}_p} f\, d\varrho_m(x)$$

for all continuous functions f (See Lemma 46) . Then we get the additional information that

$$\kappa_{2,r}(F)=\left(\int_{\mathbb{Z}_p} (1+q)^{ux}\gamma_0^n(x)\, d\mu_F(x)\right)_{n\geq 0}.$$

Again we have

Proposition 78. *For an element $k\in u+\tilde{q}\mathbb{Z}$ we write $\hat{k}:=\frac{k-u}{\tilde{q}}$. We have a commutative diagram of $\mathbb{Z}_p$-module homomorphisms*

$$\begin{tikzcd} & \mathbb{Z}_p[\![T]\!] \arrow[dl, "\kappa_{2,r}", "\sim"'] \arrow[dr, "\Gamma_r"] & \\ \mathbf{X}_{2,r} \arrow[rr, "\hat{\Gamma}_{2,r}"'] & & \prod_{\substack{k\geq 4\\ k\equiv r \bmod \tilde{q}}} \mathbb{Q}_p \end{tikzcd}$$

where

$$\hat{\Gamma}_{2,r} : \mathbf{X}_{2,r} \to \prod_{\substack{k \geq 4 \\ k \equiv r \bmod \tilde{q}}} \mathbb{Q}_p$$

is given by

$$(b_n)_{n\geq 0} \mapsto \left(\sum_{n=0}^{\hat{k}} b_n \binom{\hat{k}}{n} \right)_k .$$

Proof. Let $(b_n)_{n\geq 0} \in \mathbf{X}_{2,r}$. Regard that

$$F(\gamma_r(x)) = \sum_{n\geq 0} b_n \binom{x}{n}$$

for all $x \in \mathbb{Z}_p$ and that $\gamma_r(\hat{k}) = (1+q)^k - 1$. Therefore

$$\Gamma_r(F) = \Big(F\big((1+q)^k - 1\big) \Big)_{\substack{k \geq 4 \\ k \equiv r \bmod \tilde{q}}} = \Big(F\big(\gamma_r(\hat{k})\big) \Big)_{\substack{k \geq 4 \\ k \equiv r \bmod \tilde{q}}}$$

$$= \left(\sum_{n\geq 0} b_n \binom{\hat{k}}{n} \right)_{\substack{k \geq 4 \\ k \equiv r \bmod \tilde{q}}} = \hat{\Gamma}_{2,r}((b_n)).$$

$\square$

Corollary 79. *We have a commutative diagram of $\mathbb{Z}_p$-module homomorphisms*

$$\begin{tikzcd}
\bigoplus^*_{r\in\mathbb{Z}/\tilde{q}} \mathbb{Z}_p[\![T]\!] \arrow[rr, "\sim", "\oplus\kappa_{2,r}"'] \arrow[dr, "\Gamma"'] & & \bigoplus^*_{r\in\mathbb{Z}/\tilde{q}} \mathbf{X}_{2,r} \arrow[dl, "\hat{\Gamma}_{2,r}"] \\
& \mathbf{KC} &
\end{tikzcd}$$

where

$$\hat{\Gamma}_{2,r} : \bigoplus^*_{r\in\mathbb{Z}/\tilde{q}} \mathbf{X}_{2,r} \xrightarrow{\oplus\hat{\Gamma}_{2,r}} \bigoplus^*_{r\in\mathbb{Z}/\tilde{q}} \left(\prod_{\substack{k \geq 4 \\ k \equiv r \bmod \tilde{q}}} \mathbb{Q}_p \right) \cong \prod^*_{k\geq 4} \mathbb{Q}_p.$$

The advantage of this representation is, that now we can determine

$$\hat{\Gamma}^{-1}_{2,r} \left(\prod_{\substack{k \geq 4 \\ k \equiv r \bmod \tilde{q}}} \mathbb{Z}_{(p)} \right)$$

which will be described in a moment. The disadvantage is that until now $\mathbf{X}_{2,r}$ was not successfully determined.

Lemma 80. *Let $r \in \mathbb{Z}/\tilde{q}$ with r even. Then*

$$\mathbf{X}_{2,r} \cap c_0(\mathbb{Z}_{(p)}) = \hat{\Gamma}_{2,r}^{-1}\left(\prod_{\substack{k\geq 4 \\ k \equiv r \bmod \tilde{q}}} \mathbb{Z}_{(p)}\right).$$

Proof. Let $(b_n)_{n\geq 0} \in \mathbf{X}_{2,r} \cap c_0(\mathbb{Z}_{(p)})$. Since $\hat{k} \in \mathbb{N}_0$ we have that

$$\hat{\Gamma}_{2,r}((b_n)_{n\geq 0}) = \left(\sum_{n=0}^{\hat{k}} b_n \binom{\hat{k}}{n}\right)_k$$

is obviously an element of

$$\prod_{\substack{k\geq 4 \\ k \equiv r \bmod \tilde{q}}} \mathbb{Z}_{(p)}.$$

Assume in return that

$$(b_n)_{n\geq 0} \in \hat{\Gamma}_{2,r}^{-1}\left(\prod_{\substack{k\geq 4 \\ k \equiv r \bmod \tilde{q}}} \mathbb{Z}_{(p)}\right),$$

i.e.

$$\sum_{n=0}^{\hat{k}} b_n \binom{\hat{k}}{n} \in \mathbb{Z}_{(p)}$$

for $\hat{k} = 0, 1, 2, \ldots$. We now use induction on $\hat{k}$ to prove that $b_0, b_1, \dots \in \mathbb{Z}_{(p)}$. Obviously $b_0 \in \mathbb{Z}_{(p)}$. Assume $b_0, \ldots, b_{\hat{k}} \in \mathbb{Z}_{(p)}$. Then

$$\sum_{n=0}^{\hat{k}} b_n \binom{\hat{k}+1}{n} \in \mathbb{Z}_{(p)}.$$

Since

$$b_{\hat{k}+1} + \sum_{n=0}^{\hat{k}} b_n \binom{\hat{k}+1}{n} = \sum_{n=0}^{\hat{k}+1} b_n \binom{\hat{k}+1}{n} \in \mathbb{Z}_{(p)}$$

we get $b_{\hat{k}+1} \in \mathbb{Z}_{(p)} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)}$. □

3.5 Applications: Multiplicative string orientations

In this subsection we formulate and proof the three main results of this work. We first have to collect some results found in [AHR]. Remember that $G := \mathbb{Z}_p/\{\pm 1\}$. Again we use the $\prod^*$-notation described on page 7.

Proposition 81. *The $\mathbb{Z}_p$-module homomorphism*

$$s : M(G, \mathbb{Z}_p) \to \mathbf{KC} \subseteq \prod_{k\geq 4}^{*} \mathbb{Q}_p$$

$$\mu \mapsto \left(\int_G \bar{x}^k d\mu(\bar{x}) \right)^*_{k \geq 4}$$

is bijective. The $\mathbb{Z}_p$-module homomorphism

$$\Gamma : \bigoplus_{r \in \mathbb{Z}/\tilde{q}}^{*} \mathbb{Z}_p[\![T]\!] \xrightarrow{\sim} \mathbf{KC}$$

is therefore an isomorphism.

Proof. This is a consequence of [AHR] Proposition 9.2, Example 9.5 and Proposition 9.7. □

Remark 82. We say, a sequence

$$(z_k)^*_{k \geq 4} \in \prod_{k \geq 4}^{*} \mathbb{Q}_p$$

satisfies the generalized Kummer congruences if

$$\sum_{k \geq 4} a_k z_k \in \mathbb{Z}_p$$

for all polynomials $\sum_{k \geq 4} a_k T^k \in \mathbb{Q}_p[T]$ with the property that for all $c \in \mathbb{Z}_p^\times$ we have

$$\sum_{k \geq 4} a_k c^k \in \mathbb{Z}_p.$$

In [AHR][Proposition 9.7] it is proven, that the image **KC** of

$$s : M(G, \mathbb{Z}_p) \to \prod_{k \geq 4}^{*} \mathbb{Q}_p$$

is the set of sequences satisfying the generalized Kummer congruences. Therefore Definition 61 deserves its name.

Further Ando-Hopkins-Rezk described a very important example of an element in $M(G, \mathbb{Z}_p)$ called the Bernoulli measure.

Proposition 83 ([AHR], Example 9.9)**.** *Let $c \in \mathbb{Z}_p^\times$ be an element which projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$. There exists a measure μ_c^{Ber} such that*

$$s(\mu_c^{Ber}) = \left(-(1 - p^{k-1})(1 - c^k) \frac{B_k}{2k} \right)^*_{k \geq 4} \in \mathbf{KC}$$

where $B_4, B_6, B_8 \dots$ are the Bernoulli numbers. Further we have

$$\int_G 1 \, d\mu_c^{Ber} = \frac{1}{2p^2} \log_p c^{p(p-1)}.$$

We use the notation

$$z_c^{Ber} := \left(z_{c,k}^{Ber} \right)^*_{k \geq 4} := s(\mu_c^{Ber})$$

and

$$F_c^{Ber} := \left(F_{c,r}^{Ber}(T) \right)^*_{r \in \mathbb{Z}/\tilde{q}} := \Phi_1(\mu_c^{Ber}) = \Gamma^{-1}\left(z_c^{Ber} \right).$$

The important result in [AHR] is stated in the first two parts of the following

Theorem 84. *Let $c \in \mathbb{Z}_p^\times$ be an element which projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$.*

i) There exists an injective map

$$\mathrm{ahr}_c : \pi_0 E_\infty(MString, KO_p^\wedge) \to M(G, \mathbb{Z}_p).$$

An element $\mu \in M(G,\mathbb{Z}_p)$ is called an Ando-Hopkins-Rezk measure for c if it is an element of

$$\mathbf{AHR}_c := \mathrm{im}\,(\mathrm{ahr}_c).$$

ii) Let $\mu \in M(G,\mathbb{Z}_p)$. We have $\mu \in \mathbf{AHR}_c$ if and only if there exists an element

$$(b_k)^*_{k\geq 4} \in \prod_{k\geq 4}^{*} \mathbb{Q}_p$$

such that

a) for all even $k \geq 4$ we have

$$s(\mu)_k = \int_G \bar{x}^k d\mu(\bar{x}) = (1-c^k)(1-p^{k-1})b_k.$$

b) for all even $k \geq 4$ we have

$$b_k \equiv -\frac{B_k}{2k} \mod \mathbb{Z}_p.$$

iii) The set $\pi_0 E_\infty(MString, KO_p^\wedge)$ is a G-set. The map ahr_c is G-equivariant.

iv) Assume c fulfil the additional property to be an element of $\mathbb{Z}_{(p)}$. Then the image $\mathbf{AHR}_c^{loc}$ of the map

$$\pi_0 E_\infty(MString, KO_{(p)}) \xrightarrow{\subseteq} \pi_0 E_\infty(MString, KO_p^\wedge) \xrightarrow{\mathrm{ahr}_c} \mathbf{AHR}_c$$

is given by the set of elements $\mu \in \mathbf{AHR}_c$ which satisfy the property

$$s(\mu)_k = \int_G \bar{x}^k d\mu(\bar{x}) \in \mathbb{Z}_{(p)}$$

for all even $k \geq 4$. We have

$$\mu_c^{Ber} \in \mathbf{AHR}_c^{loc}.$$

Proof. For Part i) and ii) See Diagram (7.8) and Proposition 7.10 of [AHR].
We defer the proof of Part iii) and iv) to the next section. □

p-complete string orientations of real K-theory

Let $c \in \mathbb{Z}_p^\times$ be an element which projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$. Theorem 73 implies that we have a commutative diagram of sets

$$\begin{tikzcd}
\mathbf{AHR}_c \arrow[r, "\subseteq"] & M(G,\mathbb{Z}_p) \arrow[r, "\Phi_1", "\cong"'] \arrow[d, "s"', "\cong"] & \bigoplus^{*}_{r\in\mathbb{Z}/\tilde{q}} \mathbb{Z}_p[\![T]\!] \arrow[dl, "\cong"', "\Gamma"] \\
& \mathbf{KC} &
\end{tikzcd}$$

We now describe $\mathrm{im}(s|_{\mathbf{AHR}_c})$. Remember (Definition 22) that an element $(z_k)^*_{k\geq 4} \in \mathbf{KC}$ is an element of $\mathbf{ConA_c}$ if and only if

$$z_k \in (1-c^k)\mathbb{Z}_p$$

for all k with the property that $(1-c^k) \in p\mathbb{Z}_p$.

Lemma 85. *Let $(z_k)^*_{k\geq 4} \in \mathbf{KC}$. We have $(z_k)^*_{k\geq 4} \in \mathrm{im}(s|_{\mathbf{AHR}_c})$ if and only if*

$$(z_k - z^{Ber}_{c,k})^*_{k\geq 4} \in \mathbf{ConA_c}.$$

Proof. Assume $(z_k)^*_{k\geq 4} \in \mathrm{im}(s|_{\mathbf{AHR}_c})$. Then for every even $k \geq 4$ there exists an element $b_k \in \mathbb{Q}_p$ such that

$$z_k = (1-c^k)(1-p^{k-1})b_k$$

and

$$b_k \equiv -\frac{B_k}{2k} \mod \mathbb{Z}_p.$$

This imply

$$z_k - z^{Ber}_{c,k} = (1-c^k)(1-p^{k-1})\left(b_k + \frac{B_k}{2k}\right)$$

for all even $k \geq 4$. Since $1-p^{k-1} \in \mathbb{Z}_p^\times$ this imply

$$z_k \equiv z^{Ber}_{c,k} \mod (1-c^k)\mathbb{Z}_p$$

for all even $k \geq 4$. and this imply

$$(z_k - z^{Ber}_{c,k})^*_{k\geq 4} \in \mathbf{ConA_c}.$$

Assume in return that $(z_k - z^{Ber}_{c,k})^*_{k\geq 4} \in \mathbf{ConA_c}$. This imply

$$z_k - z^{Ber}_{c,k} \in (1-c^k)\mathbb{Z}_p$$

for all k with the property that $(1-c^k) \in p\mathbb{Z}_p$. For all k with the property that $(1-c^k) \notin p\mathbb{Z}_p$ we have that $(1-c^k)\mathbb{Z}_p = \mathbb{Z}_p$. Regard that $(z_k)^*_{k\geq 4} \in \mathbf{KC}$ imply $z_k \in \mathbb{Z}_p$ for all even $k \geq 4$. Therefore

$$z_k - z^{Ber}_{c,k} \in (1-c^k)\mathbb{Z}_p$$

for all even $k \geq 4$. Then there exits elements $l_k \in \mathbb{Z}_p$ such that

$$z_k = (1-c^k)(1-p^{k-1})l_k + z^{Ber}_{c,k}$$

for all even $k \geq 4$. This imply that

$$z_k = (1-c^k)(1-p^{k-1})\left(l_k - \frac{B_k}{2k}\right)$$

for all even $k \geq 4$. This imply $(z_k)^*_{k\geq 4} \in \mathrm{im}(s|_{\mathbf{AHR}_c})$.

□

Theorem 86 (Theorem A)**.** *Let $c \in \mathbb{Z}_p^\times$ be an element which projects to a generator of $G = \mathbb{Z}_p^\times/\{\pm 1\}$. We take an arbitrary element*

$$(F_r)^*_{r\in\mathbb{Z}/\tilde{q}} \in \left(T\mathbb{Z}_p[\![T]\!] \oplus \bigoplus_{r\in(\mathbb{Z}/\tilde{q})-\{0\}}^{*} \mathbb{Z}_p[\![T]\!] \right).$$

Then there exists a unique measure $\mu \in \mathbf{AHR}_c$ such that

$$\int_G \bar{x}^k d\mu(\bar{x}) = F_k\big((1+q)^k - 1\big) - (1-c^k)(1-p^{k-1})\frac{B_k}{2k}.$$

Moreover the map

$$\left(T\mathbb{Z}_p[\![T]\!] \oplus \bigoplus_{r\in(\mathbb{Z}/\tilde{q})-\{0\}}^{*} \mathbb{Z}_p[\![T]\!] \right) \xrightarrow{\sim} \mathbf{AHR}_c \cong \pi_0 E_\infty(MString, KO_p^\wedge)$$

$$(F_r)^*_{r\in\mathbb{Z}/\tilde{q}} \mapsto \mu$$

is a bijection.

Proof. We use the commutative diagram

$$\begin{tikzcd}
\mathbf{AHR}_c \arrow[r, "\subseteq"] & M(G,\mathbb{Z}_p) \arrow[r, "\Phi_1", "\cong"'] \arrow[d, "s"', "\cong"] & \bigoplus^{*}_{r\in\mathbb{Z}/\tilde{q}} \mathbb{Z}_p[\![T]\!] \arrow[dl, "\cong", "\Gamma"'] \\
& \mathbf{KC} &
\end{tikzcd}$$

Lemma 85 imply that

$$\operatorname{im}(s|_{\mathbf{AHR}_c}) = (z^{Ber}_{c,k})^*_{k\geq 4} + \mathbf{ConA}_c.$$

Therefore we have

$$\Phi_1(\mathbf{AHR}_c) = \Gamma^{-1}\Big((z^{Ber}_k)^*_{k\geq 4}\Big) + \Gamma^{-1}(\mathbf{ConA}_c) = F^{Ber}_c + \Gamma^{-1}(\mathbf{ConA}_c).$$

Therefore we get a bijection

$$\varphi : \Gamma^{-1}(\mathbf{ConA_c}) \xrightarrow{\cong} F^{Ber}_c + \Gamma^{-1}(\mathbf{ConA_c}) \xrightarrow{\Phi_1^{-1}} \mathbf{AHR}_c.$$

Proposition 28 states that

$$\Gamma^{-1}(\mathbf{ConA_c}) = \left\{ (F_r)^*_{r\in\mathbb{Z}/\tilde{q}} \in \bigoplus_{r\in\mathbb{Z}/\tilde{q}}^{*} \mathbb{Z}_p[\![T]\!] \;\middle|\; F_0(0) = 0 \right\}$$

$$= \left(T\mathbb{Z}_p[\![T]\!] \oplus \bigoplus_{r\in(\mathbb{Z}/\tilde{q})-\{0\}}^{*} \mathbb{Z}_p[\![T]\!] \right).$$

Let

$$(F_r)^*_{r\in\mathbb{Z}/\tilde{q}} \in \left(T\mathbb{Z}_p[\![T]\!] \oplus \bigoplus_{r\in(\mathbb{Z}/\tilde{q})-\{0\}}^{*} \mathbb{Z}_p[\![T]\!] \right)$$

and let
$$\mu := \varphi\big((F_r)^*_{r\in\mathbb{Z}/\tilde{q}}\big) = \Phi_1^{-1}\Big(F_c^{Ber} + (F_r)^*_{r\in\mathbb{Z}/\tilde{q}}\Big).$$
Therefore we have
$$\begin{aligned}\left(\int_G \bar{x}^k d\mu(\bar{x})\right)^*_{k\geq 4} &= s(\mu) = \Gamma\Big(F_c^{Ber} + (F_r)^*_{r\in\mathbb{Z}/\tilde{q}}\Big)\\ &= (z^{Ber}_{c,k})^*_{k\geq 4} + \Big(F_k\big((1+q)^k-1\big)\Big)^*_{k\geq 4}\\ &= \left(-(1-c^k)(1-p^{k-1})\frac{B_k}{2k} + F_k\big((1+q)^k-1\big)\right)^*_{k\geq 4}.\end{aligned}$$
This proves the Theorem.

□

The quotient of the G-action

Remember that Theorem 84 states that $\pi_0 E_\infty(MString, KO_p^\wedge)$ carries the structure of an G-set. The equivalence relation given by the G-action is denoted by $\sim_G$. The goal of this section is to prove

Theorem 87 (Theorem B)**.** *The quotient set*
$$\pi_0 E_\infty(MString, KO_p^\wedge)/\sim_G$$
contains uncountable many elements.

Therefore we show that there exists an injective map
$$\mathbb{Z}_p[\![T]\!] \hookrightarrow \pi_0 E_\infty(MString, KO_p^\wedge)/\sim_G .$$
Let $c\in\mathbb{Z}_p^\times$ be an element which projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$ and which satisfies
$$l_c := \frac{1}{2p^2}\log_p c^{p(p-1)} = 1$$
(the existence of such an element is proven in Lemma 20). Theorem 84 and Proposition 72 states that the map
$$\Phi_c = (\Phi_1\circ \mathrm{ahr}_c) : \pi_0 E_\infty(MString, KO_p^\wedge) \hookrightarrow \bigoplus^*_{r\in\mathbb{Z}/\tilde{q}} \mathbb{Z}_p[\![T]\!]$$
is G-equivariant. Lemma 85 imply that the image of Φ_c is given by the set
$$\begin{aligned}&\Big(F^{Ber}_{c,r}(T)\Big)^*_{r\in\mathbb{Z}/\tilde{q}} + \left(T\mathbb{Z}_p[\![T]\!] \oplus \bigoplus^*_{r\in(\mathbb{Z}/\tilde{q})-\{0\}} \mathbb{Z}_p[\![T]\!]\right)\\ &= \big(F^{Ber}_{0,0}(0) + T\mathbb{Z}_p[\![T]\!]\big) \oplus \bigoplus^*_{r\in(\mathbb{Z}/\tilde{q})-\{0\}} \mathbb{Z}_p[\![T]\!]\end{aligned}$$
and this set is therefore a G-invariant subset. Proposition 72 and Proposition 83 imply
$$F^{Ber}_{0,0}(0) = l_c = 1.$$

Remember that Lemma 69 states that there is a $\Delta \times \mathbb{Z}_p$-action

$$(\Delta \times \mathbb{Z}_p) \times \bigoplus_{\theta \in \widehat{\Delta}} \mathbb{Z}_p[\![T]\!] \to \bigoplus_{\theta \in \widehat{\Delta}} \mathbb{Z}_p[\![T]\!]$$

$$((\xi, \lambda), (F_\theta)_{\theta \in \widehat{\Delta}}) \mapsto (\xi, \lambda) \odot (F_\theta)_{\theta \in \widehat{\Delta}} := \Big(\theta(\xi)(\lambda \odot F_\theta)\Big)_{\theta \in \widehat{\Delta}}$$

where $\lambda \odot F_\theta(T) = (1+T)^\lambda F_\theta(T)$. Together with the isomorphism of topological groups

$$G = \mathbb{Z}_p^\times / \{\pm 1\} \to \Delta \times \mathbb{Z}_p$$

described in Lemma 11 and the canonical isomorphism

$$\overset{*}{\bigoplus_{r \in \mathbb{Z}/\tilde{q}}} \mathbb{Z}_p[\![T]\!] \xrightarrow{\sim} \bigoplus_{\theta \in \widehat{\Delta}} \mathbb{Z}_p[\![T]\!]$$

$$(F_r) \mapsto (F_{\omega^r})$$

this $\Delta \times \mathbb{Z}_p$-action defines the G-action on

$$\overset{*}{\bigoplus_{r \in \mathbb{Z}/\tilde{q}}} \mathbb{Z}_p[\![T]\!].$$

Therefore we have a canonical bijection between the sets

$$\pi_0 E_\infty(MString, KO_p^\wedge)/\sim_G \;\cong \left((1 + T\mathbb{Z}_p[\![T]\!]) \oplus \overset{*}{\bigoplus_{r \in (\mathbb{Z}/\tilde{q}) - \{0\}}} \mathbb{Z}_p[\![T]\!] \right) \Big/ \sim_G$$

and

$$\left((1 + T\mathbb{Z}_p[\![T]\!]) \oplus \bigoplus_{\theta \in \widehat{\Delta} - \{1\}} \mathbb{Z}_p[\![T]\!] \right) \Big/ \sim_{\Delta \times \mathbb{Z}_p} .$$

Proposition 56 states that there exists a bijection

$$\mathbb{Z}_p[\![T]\!] \xrightarrow{\sim} (1 + T\mathbb{Z}_p[\![T]\!]) / \sim_{\mathbb{Z}_p} .$$

Therefore Theorem B is implied by the following

Proposition 88. *The map*

$$\varphi : (1 + T\mathbb{Z}_p[\![T]\!]) / \sim_{\mathbb{Z}_p} \hookrightarrow \left((1 + T\mathbb{Z}_p[\![T]\!]) \oplus \bigoplus_{\theta \in \widehat{\Delta} - \{1\}} \mathbb{Z}_p[\![T]\!] \right) \Big/ \sim_{\Delta \times \mathbb{Z}_p}$$

$$[F]_{\sim_{\mathbb{Z}_p}} \mapsto [(H_\theta)_{\theta \in \widehat{\Delta}}]_{\sim_{\Delta \times \mathbb{Z}_p}}$$

where

$$H_\theta = \begin{cases} F & \text{if } \theta = 1 \\ 0 & \text{else} \end{cases}$$

is a well-defined injection.

Proof. Let
$$[F]_{\sim_{\mathbb{Z}_p}}, [\tilde{F}]_{\sim_{\mathbb{Z}_p}} \in (1+T\mathbb{Z}_p[\![T]\!]) \,/ \sim_{\mathbb{Z}_p} .$$
Let
$$[(H_\theta)_{\theta\in\widehat{\Delta}}]_{\sim_{\Delta\times\mathbb{Z}_p}} := \varphi([F]_{\sim_{\mathbb{Z}_p}}) \text{ and } [(\tilde{H}_\theta)_{\theta\in\widehat{\Delta}}]_{\sim_{\Delta\times\mathbb{Z}_p}} := \varphi([\tilde{F}]_{\sim_{\mathbb{Z}_p}}).$$
We have
$$[(H_\theta)_{\theta\in\widehat{\Delta}}]_{\sim_{\Delta\times\mathbb{Z}_p}} = [(\tilde{H}_\theta)_{\theta\in\widehat{\Delta}}]_{\sim_{\Delta\times\mathbb{Z}_p}}$$
if and only if there exists a $(\xi,\lambda)\in\Delta\times\mathbb{Z}_p$ such that
$$(\xi,\lambda)\otimes(H_\theta)_{\theta\in\widehat{\Delta}} = \big(\theta(\xi)(1+T)^\lambda H_\theta\big)_{\theta\in\widehat{\Delta}}.$$
Since $H_\theta = \tilde{H}_\theta = 0$ for all $\theta\in\widehat{\Delta}-\{1\}$, this is equivalent to
$$\tilde{F} = \tilde{H}_1 = (1+T)^\lambda H_1 = (1+T)^\lambda F$$
and this is equivalent to
$$[F]_{\sim_{\mathbb{Z}_p}} = [\tilde{F}]_{\sim_{\mathbb{Z}_p}}.$$
Therefore the map is well defined and injective. □

p-local string orientations of real K-theory

Remember (Theorem 84) that we have a bijection
$$\mathrm{ahr}_c^{-1}|_{\mathbf{AHR}_c^{loc}} : \mathbf{AHR}_c^{loc} \xrightarrow{\cong} \pi_0 E_\infty(MString, KO_{(p)}).$$
The goal of this paragraph is to prove

Theorem 89 (Theorem C)**.** *Let $c\in\mathbb{Z}_{(p)}\subseteq\mathbb{Z}_p^\times$ be an element which projects to a generator of $\mathbb{Z}_p^\times/\{\pm1\}$. With $\mathbf{Y}\subseteq c_0(\mathbb{Z}_p)$ we denote the subset of elements $(b_n)_{n\geq0}\in c_0(\mathbb{Z}_p)$ which fulfil the following properties:*

i) For all $n\geq0$ we have $b_n\in\mathbb{Z}_{(p)}$.

ii) For all $n\geq0$ we have
$$\frac{b_n}{n!p^n}\in\mathbb{Z}_p.$$

Let
$$\mathbf{Y}_0 := \{(b_n)_{n\geq0}\in\mathbf{Y} \mid b_0=0\}.$$
and let $\hat{p}_k := p^{-1}\big((1+q)^k-1\big)$. We take an arbitrary element
$$\Big((b_{r,n})_{n\geq0}\Big)^*_{r\in\mathbb{Z}/\tilde{q}} \in \left(\mathbf{Y}_0 \oplus \bigoplus_{r\in(\mathbb{Z}/\tilde{q})-\{0\}}^{*} \mathbf{Y}\right).$$
Then there exists an unique measure $\mu\in\mathbf{AHR}_c^{loc}$ such that
$$\int_G \bar{x}^k d\mu(\bar{x}) = \left(\sum_{n=0}^{\hat{p}_k} b_{k,n}\binom{\hat{p}_k}{n}\right) - (1-c^k)(1-p^{k-1})\frac{B_k}{2k}.$$

Moreover the map

$$\left(\mathbf{Y}_0 \oplus \bigoplus_{r\in(\mathbb{Z}/\tilde{q})-\{0\}}^{*} \mathbf{Y}\right) \hookrightarrow \mathbf{AHR}_c^{loc} \cong \pi_0 E_\infty(MString, KO_{(p)})$$

$$\Big((b_{r,n})_{n\geq 0}\Big)^{*}_{r\in\mathbb{Z}/\tilde{q}} \mapsto \mu$$

is an injection.

Proof. Let

$$\Big((b_{r,n})_{n\geq 0}\Big)^{*}_{r\in\mathbb{Z}/\tilde{q}} \in \left(\mathbf{Y}_0 \oplus \bigoplus_{r\in(\mathbb{Z}/\tilde{q})-\{0\}}^{*} \mathbf{Y}\right).$$

Proposition 74 imply that we have a commutative diagram of $\mathbb{Z}_p$-modules

$$\begin{tikzcd} \bigoplus\limits_{r\in\mathbb{Z}/\tilde{q}}^{*} \mathbb{Z}_p[\![T]\!] \arrow[r, "\oplus\kappa_1", "\cong"'] \arrow[d, "\Gamma"', "\cong"] & \bigoplus\limits_{r\in\mathbb{Z}/\tilde{q}}^{*} \mathbf{X}_1 \arrow[dl, "\cong"', "\hat{\Gamma}_1"] \\ \mathbf{KC} & \end{tikzcd}$$

Let $\mathbf{X}_{1,0} := \{(b_n)_{n\geq 0} \in \mathbf{X}_1 \mid b_0 = 0\}$. Part ii) of Lemma 76 imply that we have a commutative diagram

$$\begin{tikzcd} \left(\mathbf{Y}_0 \oplus \bigoplus\limits_{r\in(\mathbb{Z}/\tilde{q})-\{0\}}^{*} \mathbf{Y}\right) \arrow[r, "\subseteq"] & \left(\mathbf{X}_{1,0} \oplus \bigoplus\limits_{r\in(\mathbb{Z}/\tilde{q})-\{0\}}^{*} \mathbf{X}_1\right) \arrow[r, "\oplus\kappa_1^{-1}", "\cong"'] \arrow[d, "\hat{\Gamma}_1"'] & \left(T\mathbb{Z}_p[\![T]\!] \oplus \bigoplus\limits_{r\in(\mathbb{Z}/\tilde{q})-\{0\}}^{*} \mathbb{Z}_p[\![T]\!]\right) \arrow[dl, "\Gamma"] \\ & \mathbf{KC} & \end{tikzcd}$$

We define $\mu \in \mathbf{AHR}_c$ to be the measure described in Theorem A (Theorem 86) which corresponds to the element

$$(F_r)^{*}_{r\in\mathbb{Z}/\tilde{q}} := (\oplus\kappa_1^{-1})\left(\Big((b_{r,n})_{n\geq 0}\Big)^{*}_{r\in\mathbb{Z}/\tilde{q}}\right) \in \left(T\mathbb{Z}_p[\![T]\!] \oplus \bigoplus_{r\in(\mathbb{Z}/\tilde{q})-\{0\}}^{*} \mathbb{Z}_p[\![T]\!]\right).$$

Remember that Proposition 74 states that

$$F_k\big((1+q)^k - 1\big) = \sum_{n=0}^{\hat{p}_k} \binom{\hat{p}_k}{n} b_{k,n}.$$

Theorem A states that

$$\begin{aligned} \int_G \bar{x}^k d\mu(\bar{x}) &= F_k\big((1+q)^k - 1\big) - (1-c^k)(1-p^{k-1})\frac{B_k}{2k} \\ &= \left(\sum_{n=0}^{\hat{p}_k} \binom{\hat{p}_k}{n} b_{k,n}\right) - (1-c^k)(1-p^{k-1})\frac{B_k}{2k} \end{aligned}$$

for all even $k \geq 4$. Now we prove that $\mu \in \mathbf{AHR}_c^{loc}$. Part iv) of Theorem 84 states that $\mu_c^{Ber} \in \mathbf{AHR}_c^{loc}$. Therefore we have

$$s(\mu_c^{Ber})_k = -(1-c^k)(1-p^{k-1})\frac{B_k}{2k} \in \mathbb{Z}_{(p)}$$

for all even $k \geq 4$. Since $b_{k,n} \in \mathbb{Z}_{(p)}$ for all $n \geq 0$ and all even $k \geq 4$ we have that

$$\left(\sum_{n=0}^{\hat{p}_k} \binom{\hat{p}_k}{n} b_{k,n}\right) \in \mathbb{Z}_{(p)}.$$

All together we get that

$$\int_G \bar{x}^k d\mu(\bar{x}) \in \mathbb{Z}_{(p)}$$

for all even $k \geq 4$. Therefore Part iv) of Theorem 84 implies that

$$\mu \in \mathbf{AHR}_c^{loc}.$$

□

4 Measures and E_∞ orientations for $K(1)$-local spectra

The whole section we fix a prime p and we write

$$G := \mathbb{Z}_p^\times/\{\pm 1\}.$$

Let $c \in \mathbb{Z}_p^\times$ be an element which projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$. Remember that we deferred the proof of Theorem 84 which stated that

i) There exists an injective map

$$\mathrm{ahr}_c : \pi_0 E_\infty(MString, KO_p^\wedge) \to M(G, \mathbb{Z}_p).$$

ii) Let $\mu \in M(G, \mathbb{Z}_p)$. We have $\mu \in \mathbf{AHR}_c := \mathrm{im}(\mathrm{ahr}_c)$ if and only if there exists an element

$$(b_k)^*_{k\geq 4} \in \prod_{\substack{k\geq 4\\ k \text{ even}}} \mathbb{Q}_p$$

such that

a) for all even $k \geq 4$ we have

$$\int_G \bar{x}^k d\mu(\bar{x}) = (1-c^k)(1-p^{k-1})b_k.$$

b) for all even $k \geq 4$ we have

$$b_k \equiv -\frac{B_k}{2k} \mod \mathbb{Z}_p.$$

iii) The set $\pi_0 E_\infty(MString, KO_p^\wedge)$ is a G-set. The map

$$\mathrm{ahr}_c : \pi_0 E_\infty(MString, KO_p^\wedge) \to M(G, \mathbb{Z}_p)$$

is G-equivariant.

iv) Assume c fulfil the additional property to be an element of $\mathbb{Z}_{(p)}$. Then the image $\mathbf{AHR}_c^{loc}$ of the map

$$\pi_0 E_\infty(MString, KO_{(p)}) \xrightarrow{\subseteq} \pi_0 E_\infty(MString, KO_p^\wedge) \xrightarrow{\mathrm{ahr}_c} \mathbf{AHR}_c$$

is given by the set of elements $\mu \in \mathbf{AHR}_c$ which satisfy the property

$$\int_G \bar{x}^k d\mu(\bar{x}) \in \mathbb{Z}_{(p)}$$

for all even $k \geq 4$. We have

$$\mu_c^{Ber} \in \mathbf{AHR}_c^{loc}.$$

The first two parts are already shown in [AHR]. The goal of this section is to prove the last two parts. Therefore we have to repeat large parts of the constructions made in [AHR]. We show that there exists sets $\pi_0\mathbf{A}(gl_1 KO_p^\wedge)$, $\pi_0\mathbf{A}(KO_p^\wedge)$, $\pi_0\mathbf{B}(KO_p^\wedge)$ and five maps (of sets)

$$\eta_1 : \pi_0 E_\infty(MString, KO_p^\wedge) \longrightarrow \pi_0\mathbf{A}(gl_1 KO_p^\wedge)$$

$$\eta_2 : \pi_0\mathbf{A}(gl_1 KO_p^\wedge) \longrightarrow \pi_0\mathbf{A}(KO_p^\wedge)$$
$$\eta_3 : \pi_0\mathbf{A}(KO_p^\wedge) \longrightarrow \pi_0\mathbf{B}(KO_p^\wedge)$$
$$\eta_4 := \eta_{4,c} : \pi_0\mathbf{B}(KO_p^\wedge) \longrightarrow [KO_p^\wedge, KO_p^\wedge]$$
$$\eta_5 : [KO_p^\wedge, KO_p^\wedge] \longrightarrow M(G, \mathbb{Z}_p).$$

Then we show that every appearing set carries the structure of a G-set and we show that $\eta_1, \ldots, \eta_5$ are G-equivariant. In [AHR] it is shown that the maps η_1, η_2, η_3 and η_5 are bijections and that η_4 is injective. The last part of this section is to prove part iv) by using arithmetic squares.

4.1 Obstruction theory following Ando-Hopkins-Rezk

Remember that our goal is to describe the maps $\eta_1, \ldots, \eta_5$ on page 67. The main tool for doing this is described in the next paragraph.

Functors and automorphisms of p-complete real K-Theory

Let $\mathcal{KO}$ be the category whose only object is $KO_p^\wedge$ and whose set of morphisms is given by the set of automorphisms

$$\{\psi^g : KO_p^\wedge \to KO_p^\wedge \mid g \in G\}$$

where ψ^g is the Adams operation at g. Then we have the following

Lemma 90. *Let $\mathcal{C}$ be a category, such that $\mathcal{KO}$ is a subcategory of $\mathcal{C}$.*

i) Let

$$\mathbf{F} : \mathcal{C} \to \text{sets}$$

be a functor. Then the set $\mathbf{F}(KO_p^\wedge)$ carries the structure of a G-set.

ii) Let

$$\mathbf{G} : \mathcal{C} \to \text{sets}$$

be another functor and assume that there is a natural transformation η for $\mathbf{F}$ to $\mathbf{G}$. Then the map

$$\eta_{KO_p^\wedge} : \mathbf{F}(KO_p^\wedge) \to \mathbf{G}(KO_p^\wedge)$$

is G-equivariant.

Proof. Let $g \in G$ and ψ^g the Adams operation at g. The map

$$\varphi_{\mathbf{F}} : G \to \mathrm{Aut}(\mathbf{F}(KO_p^\wedge))$$
$$g \mapsto \mathbf{F}(\psi^g)$$

defines a G-action on $\mathbf{F}(KO_p^\wedge)$. The natural transformation η induces a map

$$\mathrm{im}(\varphi_{\mathbf{F}}) \to \mathrm{im}(\varphi_{\mathbf{G}})$$
$$\mathbf{F}(\psi^g) \mapsto \mathbf{G}(\psi^g).$$

Obviously the diagram

$$\begin{tikzcd} & G \arrow[dl] \arrow[dr] & \\ \mathrm{im}(\varphi_{\mathbf{F}}) \arrow[rr] & & \mathrm{im}(\varphi_{\mathbf{G}}) \end{tikzcd}$$

commutes, and therefore $\eta_{KO_p^\wedge}$ is G-equivariant. $\square$

We now start to repeat the construction of the functors $\pi_0\mathbf{A}(-)$ and $\pi_0\mathbf{B}(-)$. The first step to attack the problem of understanding $\pi_0 E_\infty(MString, KO_p^\wedge)$ is to convert this to problem regarding spectra not E_∞-spectra. Therefore Ando-Hopkins-Rezk used the space of units of a ring spectrum.

Units of ring spectra following May-Quinn-Ray

Definition 91. Let R be a ring spectrum (i.e. an algebra object in the symmetric monoidal category $(\text{spectra}, \wedge, S)$). The pull-back GL_1R in the diagram

$$\begin{tikzcd} GL_1R \arrow[r] \arrow[d] & \Omega^\infty R \arrow[d] \\ (\pi_0 R)^\times \arrow[r] & \pi_0 R \end{tikzcd}$$

is called the space of units of R.

If R is an E_∞ spectrum, then J. P. May, F. Quinn and N. Ray proved that there exists a (-1)-connected spectrum gl_1R such that

$$GL_1R \approx \Omega^\infty gl_1R.$$

A construction of this spectrum can be found for example in Section 3 of [ABGHR]. Theorem 3.2 in [ABGHR] states, that there is an adjunction

$$\Sigma^\infty_+\Omega^\infty : \mathrm{Ho}((-1)-\textit{connected spectra}) \rightleftarrows \mathrm{Ho}\ E_\infty-\textit{spectra} :\ gl_1.$$

Example 92. We have

$$\pi_0\ gl_1S = \pi_0\ GL_1S = (\pi_0S)^\times = \mathbb{Z}^\times = \{\pm 1\}.$$

If X is a space, then

$$[X, GL_1R] = \tilde{R}^0(X)^\times$$

and if X is a pointed space, then

$$[X, GL_1R]_+ = (1 + \tilde{R}^0(X))^\times \subseteq \tilde{R}^0(X)^\times$$

(This is Proposition 2.4 in [R]). Let $\text{spectra}_{/gl_1S}$ be the category of spectra under gl_1S. An object in this category is a spectrum b together with a map of spectra $gl_1S \to b$. A morphism between objects b and $\tilde{b}$ is a morphism of spectra $b \to \tilde{b}$ such that the diagram

$$\begin{tikzcd} b \arrow[rr] & & \tilde{b} \\ & gl_1S \arrow[ul] \arrow[ur] & \end{tikzcd}$$

commutes. If R is an E_∞ spectrum with unit $\iota : S \to R$ then the corresponding map

$$gl_1\iota : gl_1S \to gl_1R$$

gives gl_1R the structure of a spectrum under gl_1S. Therefore we have a functor

$$gl_1(-) : \text{Ho}\ E_\infty-\text{spectra} \to \text{Ho}\ \text{spectra}_{/gl_1S}.$$

Thom spectra

We are now interested in spectra over $bgl_1S = \Sigma gl_1S$. For them we can define the corresponding Thom spectrum.

Definition 93 ([ABGHR], Definition 2.6)**.** The Thom spectrum of $f : b \to bgl_1S$ is the homotopy push-out $M = Mf$ in the diagram of E_∞ spectra

$$\begin{tikzcd} \Sigma^\infty_+\Omega^\infty(gl_1S) \arrow[r] \arrow[d] & S \arrow[d] \\ \Sigma^\infty_+\Omega^\infty(Cf) \arrow[r] & M \end{tikzcd}$$

where Cf denotes the cofibre of $\Sigma^{-1}f : \Sigma^{-1}b \to gl_1S$. The top map is the co-unit of the adjunction $(\Sigma^\infty_+\Omega^\infty, gl_1)$.

After applying the functor $E_\infty(-, R)$ to this definition and using the adjunction $(\Sigma^\infty_+\Omega^\infty, gl_1)$ twice, we get the following

Lemma 94 ([AHR], Diagram 2.8)**.** *Let R be an E_∞ spectrum with unit $\iota : S \to R$. Let M be the Thom spectrum of $f : b \to bgl_1S$. Then $E_\infty(M, R)$ is naturally weakly equivalent to the homotopy pull-back in the diagram*

$$\begin{tikzcd} E_\infty(M, R) \arrow[r] \arrow[d] & \text{spectra}(gl_1S/Cf, gl_1R) \arrow[d] \\ \{gl_1\iota\} \arrow[r] & \text{spectra}(gl_1S, gl_1R). \end{tikzcd}$$

Example 95. Let bo and bu denote the connective real and complex K-theory spectrum. By the j-homomorphism $j : bo \to bgl_1S$ respectively $j : bu \to bgl_1S$ they are spectra over bgl_1S. Therefore the associated spectra $bo\langle 2n\rangle$ and $bu\langle 2n\rangle$ are spectra over bgl_1S for all non-negative integers k. We use the notation $o\langle 2n\rangle := \Sigma^{-1}bo\langle 2n\rangle$ and denote the cofibre of

$$\Sigma^{-1}j : o\langle 2n\rangle \to gl_1S$$

by $gl_1S/o\langle 2n\rangle$ and the Thom spectrum of $j : bo\langle 2n\rangle \to bgl_1S$ by $MO\langle 2n\rangle$. In [ABGHR, §8] it is shown that the spectrum underlying $M(f : b \to bgl_1S)$ is the usual Thom spectrum of the spherical fibration classified by $\Omega^\infty f : B \to BGL_1S$. Thus $MO\langle 2n\rangle$ coincides with the usual definition of Thom spectra. Further the following notations are used:

$$bstring := bo\langle 8\rangle\,; \quad string := o\langle 8\rangle, \quad MString := MO\langle 8\rangle.$$

Corollary 96. *Let $\iota : S \to R$ denote the unit of the E_∞ spectrum R. The space $E_\infty(MO\langle 2n\rangle, R)$ is naturally weakly equivalent to the homotopy pull-back in the diagram*

$$\begin{tikzcd} E_\infty(MO\langle 2n\rangle, R) \arrow[r] \arrow[d] & \text{spectra}(gl_1S/o\langle 2n\rangle, gl_1R) \arrow[d] \\ \{gl_1\iota\} \arrow[r] & \text{spectra}(gl_1S, gl_1R) \end{tikzcd}$$

for all non-negative integers n.

The obstruction

Corollary 96 motivates the following

Definition 97 ([AHR], Definition 5.3)**.** Let

$$\mathbf{A} : \text{Ho spectra}_{/gl_1 S} \to \text{spaces}$$

be the functor which maps a spectrum

$$i : gl_1 S \to X$$

to the homotopy pull-back in the diagram

$$\begin{tikzcd} \mathbf{A}(X) \arrow[r] \arrow[d] & \text{spectra}(gl_1 S/string, X) \arrow[d] \\ \{i\} \arrow[r] & \text{spectra}(gl_1 S, X) \end{tikzcd}$$

The diagram induces a long exact sequence

$$\cdots \to \pi_0 \mathbf{A}(X) \to [gl_1 S/string, X] \to [gl_1 S, X] \to 0 \tag{98}$$

which tells us, that $\pi_0 \mathbf{A}(X)$ is non-empty if and only if there exists a map

$$u : gl_1 S/string \to X$$

making the diagram

$$\begin{tikzcd} string \arrow[r, "j"] & gl_1 S \arrow[r, "\pi"] \arrow[dr, "i"'] & gl_1 S/string \arrow[r] \arrow[d, dotted, "u"] & bstring \\ & & X & \end{tikzcd}$$

commutative up to homotopy and this happens if and only if the map

$$string \xrightarrow{j} gl_1 S \xrightarrow{i} X$$

is nullhomotopic.

Definition 99 ([AHR], Paragraph 5.1)**.** Let

$$\mathbf{B} : \text{Ho spectra}_{/gl_1 S} \to \text{sets}$$

be the functor which maps an object $i : gl_1 S \to X$ to image of the map

$$\pi_0 \mathbf{A}(X) \to [gl_1 S/string, X]$$

which is occurs in sequence 98.

Then we get

Proposition 100. *The sets $\pi_0 E_\infty(MString, KO_p^\wedge)$ and $\pi_0\mathbf{A}(gl_1(KO_p^\wedge))$ are G-sets. There exists an equivariant map*

$$\eta_1 : \pi_0 E_\infty(MString, KO_p^\wedge) \longrightarrow \pi_0\mathbf{A}(gl_1(KO_p^\wedge)).$$

Proof. It is known that $\mathcal{KO}$ is a subcategory of $\text{Ho } E_\infty\text{−spectra}$. Consider the functors

$$\pi_0 E_\infty(MString, -) : \text{Ho } E_\infty\text{−spectra} \to \text{sets}.$$

and

$$\pi_0\mathbf{A}(gl_1(-)) : \text{Ho } E_\infty\text{−spectra} \to \text{sets}.$$

Corollary 96 together with Definition 97 implies that there exists a natural equivalence η_1 between these two functors. Lemma 90 states that the sets $\pi_0 E_\infty(MString, KO_p^\wedge)$ and $\pi_0\mathbf{A}(gl_1(KO_p^\wedge))$ are G-sets and that

$$\eta_1 := (\eta_1)_{KO_p^\wedge} : \pi_0 E_\infty(MString, KO_p^\wedge) \longrightarrow \pi_0\mathbf{A}(gl_1(KO_p^\wedge))$$

is G-equivariant. $\square$

The following Proposition is needed for the announced construction (see page 67) of the map η_4, which will be presented in the next subsection.

Proposition 101. *There exists a natural transformation from the functor*

$$\pi_0\mathbf{A}(-) : \text{Ho spectra}_{/gl_1 S} \to \text{sets}$$

to the functor

$$\pi_0\mathbf{B}(-) : \text{Ho spectra}_{/gl_1 S} \to \text{sets}.$$

Proof. It is obvious that the map

$$\pi_0\mathbf{A}(X) \to \mathbf{B}(X) \subseteq [gl_1 S/string, X]$$

from Sequence (98) defines a natural transformation

$$\pi_0\mathbf{A}(-) \to \mathbf{B}(-)$$

since for each morphism $X \to Y$ in the category $\text{Ho spectra}_{/gl_1 S}$ the induced diagram

$$\begin{tikzcd}
\ldots \arrow[r] & \pi_0\mathbf{A}(X) \arrow[r] \arrow[d] & {[gl_1 S/string, X]} \arrow[r] \arrow[d] & {[gl_1 S, X]} \arrow[r] \arrow[d] & 0 \\
\ldots \arrow[r] & \pi_0\mathbf{A}(Y) \arrow[r] & {[gl_1 S/string, Y]} \arrow[r] & {[gl_1 S, Y]} \arrow[r] & 0
\end{tikzcd}$$

commutes. $\square$

4.2 Localization of units

Remember that we have still to describe the maps $\eta_2, \ldots, \eta_5$ on page 67. To reach this goal we need some facts about Bousfield localization and logarithmic cohomology operations, which will repeated now.

Bousfield localization

We work with a suitable category of spaces (e.g. topological spaces) , spectra and E_∞ spectra (e.g. the model of [LMSM]). It is assumed that the reader is familiar with Bousfield localization. We repeat some facts, which are necessary in the following. Let E be a spectrum. A map of spectra $f : X \to Y$ is called an E-equivalence if the induced map f_* in E-homology is an isomorphism. A spectrum X is called E-acyclic if $E \wedge X \approx *$. It is called E-local if for each E-acyclic T we have $[T, X] = 0$. A spectrum Y is called an E-localization of X if Y is E-local and $X \to Y$ is an E-equivalence. In [B79] Bousfield proved that for every spectrum X the E-localization $X \xrightarrow{\eta_E} L_E X$ exists and is unique up to homotopy. We now collect some facts about Bousfield localization:

i) Module spectra over a ring spectrum E are E-local.

ii) The localization functor L_E can be chosen to preserve E_∞ structures.

iii) L_E is idempotent: $L_E L_E \approx L_E$

iv) L_E preserves homotopy inverse limits.

v) L_E preserves cofibre sequences.

vi) Assume $E = M(\mathbb{Z}_{(p)})$, where p is a prime and $M(.)$ is the Moore spectrum. Then $L_E X \approx X_{(p)}$ is the Bousfield p-localization.

vii) Assume $E = M(\mathbb{Z}/p)$ and X is a connective spectrum. Then

$$L_E X \approx X_p^\wedge$$

where the right hand side is defined to be the homotopy limit of

$$\cdots \to X \wedge M(\mathbb{Z}/p^2) \to X \wedge M(\mathbb{Z}/p).$$

viii) Assume $E = M\mathbb{Q}$. Then $L_E X = X \wedge H\mathbb{Q} =: X \otimes \mathbb{Q}$.

Lemma 102 ([AHR], Lemma 7.1)**.** *The natural map*

$$bo\langle 8\rangle = bstring \to bo \to KO \to KO_p^\wedge$$

is a $K(1)$-localization. In particular $KO_p^\wedge$ is $K(1)$-local.

A logarithmic cohomology operation

Ando-Hopkins-Rezk used the following tool ([AHR, Theorem 4.3]).

Proposition 103. *There exists a functor (called Bousfield-Kuhn functor)*

$$\Phi : \text{Ho spaces}_* \to \text{Ho spectra}$$

such that the functors

$$L_{K(1)}(-) : \text{Ho spectra} \to \text{Ho spectra}$$

and

$$\Phi(\Omega^\infty(-)) : \text{Ho spectra} \to \text{Ho spectra}$$

are natural equivalent.

Proof. This is shown in [B79] and [B87]. □

Let R be an E_∞-spectrum and let

$$GL_1R \to \Omega^\infty R$$

be the inclusion. This induces a map

$$GL_1R\langle 1\rangle \to \Omega^\infty R\langle 1\rangle.$$

Applying the Bousfield-Kuhn functor we get a map

$$L_{K(1)}gl_1R \cong L_{K(1)}gl_1R\langle 1\rangle \to L_{K(1)}R\langle 1\rangle \cong L_{K(1)}R$$

Composition with the universal map $gl_1R \to L_{K(1)}gl_1R$ gives us a map

$$l_R : gl_1R \to L_{K(1)}R.$$

In [R] Rezk showed that this map is natural in R, i.e. we have the following

Lemma 104 (Section 3.5 in [R] or equation (4.4) in [AHR])**.** *There exists a natural transformation between the functors*

$$gl_1(-) : \text{Ho } E_\infty\text{−spectra} \to \text{Ho spectra}_{/gl_1S}$$

and

$$L_{K(1)}(-) : \text{Ho } E_\infty\text{−spectra} \to \text{Ho spectra}_{/gl_1S}\,.$$

$$R \mapsto (gl_1S \to gl_1R \xrightarrow{l_R} L_{K(1)}R).$$

Further we have the following

Lemma 105. *i) The category $\mathcal{KO}$ is a subcategory of* Ho spectra$_{/gl_1S}$.

ii) There exists a natural transformation from the functor

$$\text{id} : \text{Ho spectra}_{/gl_1S} \to \text{Ho spectra}_{/gl_1S}$$

$$(gl_1S \to R) \mapsto (gl_1S \to R)$$

to the functor

$$L_{K(1)} : \text{Ho spectra}_{/gl_1S} \to \text{Ho spectra}_{/gl_1S}$$

$$(gl_1S \to R) \mapsto (gl_1S \to R \to L_{K(1)}R)$$

where $R \to L_{K(1)}R$ is the universal map.

Proof. Part ii) is trivial since the universal map is natural. Remember that $KO_p^\wedge$ is $K(1)$-local. Therefore the universal map

$$KO_p^\wedge \to L_{K(1)}KO_p^\wedge$$

is a natural weak equivalence, i.e. an automorphism in Ho spectra. Let

$$\varphi : L_{K(1)}KO_p^\wedge \to KO_p^\wedge$$

be the inverse morphism in Ho spectra. Then we have a morphism

$$gl_1 S \to gl_1 KO_p^\wedge \xrightarrow{l_{KO_p^\wedge}} L_{K(1)} KO_p^\wedge \xrightarrow{\varphi} KO_p^\wedge$$

which gives $KO_p^\wedge$ the structure of a spectrum over $gl_1 S$. We now check that ψ_g is a morphism of spectra over $gl_1 S$ for all $g \in G$. Since the universal map $KO_p^\wedge \to L_{K(1)} KO_p^\wedge$ is natural we have a commutative diagram

$$\begin{tikzcd}
L_{K(1)} KO_p^\wedge \arrow[r, "\varphi"] \arrow[d, "L_{K(1)}\psi^g"'] & KO_p^\wedge \arrow[d, "\psi^g"] \\
L_{K(1)} KO_p^\wedge \arrow[r, "\varphi"'] & KO_p^\wedge
\end{tikzcd}$$

for all $g \in G$. Lemma 104 imply that the diagram

$$\begin{tikzcd}
 & L_{K(1)} KO_p^\wedge \arrow[dd, "L_{K(1)}\psi^g"] \\
gl_1 S \arrow[ur] \arrow[dr] & \\
 & L_{K(1)} KO_p^\wedge
\end{tikzcd}$$

commutes. This imply Part i). □

Corollary 106. *i) The sets $\pi_0 \mathbf{A}(KO_p^\wedge)$ and $\pi_0 \mathbf{B}(KO_p^\wedge)$ are G-sets.*

ii) There exists an equivariant map

$$\eta_2 : \pi_0 \mathbf{A}(gl_1(KO_p^\wedge)) \longrightarrow \pi_0 \mathbf{A}(KO_p^\wedge).$$

iii) There exists an equivariant map

$$\eta_3 : \pi_0 \mathbf{A}(KO_p^\wedge) \longrightarrow \pi_0 \mathbf{B}(KO_p^\wedge).$$

Proof. Consider the functors

$$\pi_0 \mathbf{A}(-) : \text{Ho spectra}_{/gl_1 S} \to sets$$

and

$$\pi_0 \mathbf{B}(-) : \text{Ho spectra}_{/gl_1 S} \to sets.$$

Lemma 105 states that $\mathcal{KO}$ is a subcategory of Ho spectra$_{/gl_1 S}$. Proposition 101 states that there is a natural transformation between these two functors. Therefore Lemma 90 implies Part i) and the existence of a G-equivariant map

$$\eta_3 : \pi_0 \mathbf{A}(KO_p^\wedge) \to \pi_0 \mathbf{B}(KO_p^\wedge)$$

which proves Part iii). Lemma 104 imply that there exists a natural transformation from the functor

$$\pi_0 \mathbf{A}(gl_1(-)) : \text{Ho } E_\infty\text{−spectra} \to sets$$

to

$$\pi_0\mathbf{A}(L_{K(1)}(-)) : \text{Ho } E_\infty\text{−spectra} \to \mathit{sets}$$

and Lemma 105 imply that there exists a natural transformation from the functor

$$\pi_0\mathbf{A}(-) : \text{Ho spectra}_{/gl_1S} \to \mathit{sets}$$

to

$$\pi_0\mathbf{A}(L_{K(1)}(-)) : \text{Ho spectra}_{/gl_1S} \to \mathit{sets}.$$

Lemma 90 imply the existence of G-equivariant maps

$$\zeta_1 : \pi_0\mathbf{A}(gl_1(KO_p^\wedge)) \longrightarrow \pi_0\mathbf{A}(L_{K(1)}KO_p^\wedge)$$

and

$$\zeta_2 : \pi_0\mathbf{A}(KO_p^\wedge) \longrightarrow \pi_0\mathbf{A}(L_{K(1)}KO_p^\wedge).$$

Since $KO_p^\wedge$ is $K(1)$-local we have that ζ_2 is a bijective G-equivariant map. Therefore we have a G-equivariant map defined by

$$\eta_2 : \pi_0\mathbf{A}(gl_1(KO_p^\wedge)) \xrightarrow{\zeta_1} \pi_0\mathbf{A}(L_{K(1)}KO_p^\wedge) \xrightarrow{\zeta_2^{-1}} \pi_0\mathbf{A}(KO_p^\wedge)$$

which proves Part ii). □

The Unstable Adams Conjecture

Let $c \in \mathbb{Z}_p^\times$ be a p-adic unit which projects to a generator of $G = \mathbb{Z}_p^\times/\{\pm 1\}$. We use the notation $\text{spectra}^{K(1)}_{/gl_1S}$ for the category of $K(1)$-local spectra under gl_1S. We now show that there is a natural transformation $\eta_4 = \eta_{4,c}$ between the functors

$$\mathbf{B}(-) : \text{Ho spectra}^{K(1)}_{/gl_1S} \to \text{sets}$$

and

$$[KO_p^\wedge, -] : \text{Ho spectra}^{K(1)}_{/gl_1S} \to \text{sets}.$$

Let j_c be the cofiber in

$$\mathit{string} \xrightarrow{\Sigma^{-1}(1-\psi^c)} \mathit{string} \to j_c,$$

and $J_c = \Omega^\infty j_c$. We need the Unstable Adams Conjecture which is verified in [F].

Lemma 107 ([AHR], Lemma 7.9)**.** *For every p-adic unit $c \in \mathbb{Z}_p^\times$ which projects to generator of $G = \mathbb{Z}_p^\times/\{\pm 1\}$ there exist weak equivalences*

$$A_c : J_c \xrightarrow{\sim} GL_1S$$

and

$$B_c : BString \xrightarrow{\sim} GL_1S/String$$

such that the diagram

$$\begin{tikzcd}
J_c \arrow[r] \arrow[d, "A_c"'] & BString \arrow[r, "\Omega^\infty(1-\psi^c)"] \arrow[d, "B_c"'] & BString \arrow[d, "="'] & \\
GL_1S \arrow[r] & GL_1S/String \arrow[r] & BString \arrow[r, "\Omega^\infty\Sigma j"] & BGL_1S
\end{tikzcd} \tag{108}$$

commute up to homotopy.

Recall that $L_{K(1)}bstring \approx KO_p^\wedge$. Applying the Bousfield-Kuhn functor Φ to diagram 108 we get that the diagram

$$\begin{tikzcd} j_c \arrow[r] \arrow[d, "\Phi A_c"'] & KO_p^\wedge \arrow[r, "1-\psi^c"] \arrow[d, "\Phi B_c"'] & KO_p^\wedge \arrow[d, "="'] & \\ L_{K(1)}gl_1S \arrow[r] & L_{K(1)}gl_1S/string \arrow[r] & KO_p^\wedge \arrow[r, "\Sigma j"] & L_{K(1)}bgl_1S \end{tikzcd} \tag{109}$$

commutes up to homotopy. Now assume that X is a $K(1)$-local spectrum over gl_1S and $(u : gl_1S/string \to X) \in \mathbf{B}(X)$ makes the diagram

$$\begin{tikzcd} string \arrow[r, "j"] & gl_1S \arrow[r, "\pi"] \arrow[dr, "i"] & gl_1S/string \arrow[r] \arrow[d, dotted, "u"] & bstring \\ & & X & \end{tikzcd}$$

commutative up to homotopy. Let $\tilde{\mathbf{B}}(X)$ be the set of homotopy classes of maps

$$\tilde{u} : L_{K(1)}gl_1S/string \to X$$

making the diagram

$$\begin{tikzcd} L_{K(1)}string \arrow[r, "L_{K(1)}j"] & L_{K(1)}gl_1S \arrow[r] \arrow[dr, "L_{K(1)}i"] & L_{K(1)}gl_1S/string \arrow[r] \arrow[d, dotted, "\tilde{u}"] & KO_p^\wedge \\ & & X & \end{tikzcd}$$

commutative up to homotopy. Since X is $K(1)$-local the map

$$\mathbf{B}(X) \to \tilde{\mathbf{B}}(X)$$

$$u \mapsto L_{K(1)}u$$

is a bijection. If $g : X \to Y$ is a morphism of $K(1)$-local spectra, then $L_{K(1)}g = g \in [X, Y]$ and the diagram

$$\begin{tikzcd} \mathbf{B}(X) \arrow[r, "u \mapsto L_{K(1)}u"] \arrow[d, "u \mapsto g \circ u"] & \tilde{\mathbf{B}}(X) \arrow[d, "\tilde{u} \mapsto (L_{K(1)}g) \circ \tilde{u}"] \\ \mathbf{B}(Y) \arrow[r, "u \mapsto L_{K(1)}u"] & \tilde{\mathbf{B}}(Y) \end{tikzcd}$$

is obviously commutative. Therefore the functors

$$\mathbf{B}(-) : \text{Ho spectra}^{K(1)}_{/gl_1S} \to \text{sets}$$

and

$$\tilde{\mathbf{B}}(-) : \text{Ho spectra}^{K(1)}_{/gl_1S} \to \text{sets}$$

are naturally equivalent. Because $\Phi A_c : KO_p^\wedge \xrightarrow{\sim} L_{K(1)}gl_1S/string$ is a weak equivalence, there is a natural transformation

$$\tilde{\mathbf{B}}(-) \to [KO_p^\wedge, -]$$

$$(L_{K(1)}gl_1S/string \xrightarrow{u} -) \mapsto (KO_p^\wedge \xrightarrow{\Phi A_c} L_{K(1)}gl_1S/string \xrightarrow{u} -)$$

Let η_4 be the natural transformation given by

$$\eta_4 : \mathbf{B}(-) \to \tilde{\mathbf{B}}(-) \to [KO_p^\wedge, -].$$

Then Lemma 90 imply the following

Lemma 110. *The map*

$$\eta_{4,c} := (\eta_{4,c})_{KO_p^\wedge} : \mathbf{B}(KO_p^\wedge) \to [KO_p^\wedge, KO_p^\wedge]$$

is G-equivariant.

4.3 Generalized Kummer congruences and the set $[KO_p^\wedge, KO_p^\wedge]$

Again we use the $\prod^*$-notation described on page 7. We defined a G-action on

$$\prod_{k\geq 4}^{*} \mathbb{Q}_p$$

by

$$g \odot (z_k)^*_{k\geq 4} := (g^k z_k)^*_{k\geq 4}$$

for all $g \in G := \mathbb{Z}_p^\times/\{\pm 1\}$. We now have to construct the G-equivariant map η_5. The underlying map of sets is described in [AHR].

Proposition 111. *i) There exists a bijection of sets*

$$\eta_5 : [KO_p^\wedge, KO_p^\wedge] \xrightarrow{\sim} M(G, \mathbb{Z}_p).$$

ii) The bijection η_5 is G-equivariant.

Proof. Part i) is Proposition 9.5 in [AHR] . We defer the prove of Part ii) to the first Paragraph of this subsection. □

The G-equivariant maps described in Proposition 100, Corollary 106, Lemma 110 and Proposition 111 compose to a G-equivariant map

$$\mathrm{ahr}_c : \pi_0 E_\infty(MString, KO_p^\wedge) \xrightarrow{\eta_1} \mathbf{A}(gl_1(KO_p^\wedge)) \xrightarrow{\eta_2} \mathbf{A}(KO_p^\wedge) \xrightarrow{\eta_3}$$

$$\mathbf{B}(KO_p^\wedge) \xrightarrow{\eta_4} [KO_p^\wedge, KO_p^\wedge] \xrightarrow{\eta_5} M(G, \mathbb{Z}_p)$$

These are the same constructions made in [AHR], i.e. $\eta_1, \eta_2, \eta_3, \eta_5$ are bijections and η_4 is injective, which imply the statement of Theorem 84 Part i). Further the image of ahr_c is given by the conditions described in Theorem 84 Part ii). Since ahr_c is G-equivariant the statement of Part iii) is proven. In the second and third paragraph of this subsection we prove Part iv) of Theorem 84.

Measures on $\mathbb{Z}_p^\times/\{\pm 1\}$ and the set $[KO_p^\wedge, KO_p^\wedge]$

The goal of this paragraph is to prove Proposition 111. We need the following facts:

i) For all $k = 4, 6, 8, \ldots$ the set $\pi_{2k} KO_p^\wedge$ is a free $\mathbb{Z}_p$-module of rank 1.

ii) For every element $\alpha \in [KO_p^\wedge, KO_p^\wedge]$ there exists a unique element $\lambda \in \mathbb{Z}_p$ such that
$$(\pi_{2k}\alpha)(x) = \lambda x$$
for all $k = 4, 6, 8, \ldots$. We identify λ with $\pi_{2k}\alpha$.

iii) Let $\psi^g : KO_p^\wedge \to KO_p^\wedge$ be the Adams operation at g. The automorphism
$$\pi_{2k}\psi^g : \pi_{2k} KO_p^\wedge \to \pi_{2k} KO_p^\wedge$$
is given by
$$x \mapsto g^k x$$
for all $g \in G$ and for all $k = 4, 6, 8, \ldots$.

Further we have

Proposition 112 ([AHR], Proposition 9.7)**.** *The natural map*
$$\tilde{s} : [KO_p^\wedge, KO_p^\wedge] \to \prod_{k \geq 4}^{*} \mathbb{Q}_p$$
$$\alpha \mapsto (\pi_{2k}\alpha)^*_{k \geq 4}$$
is injective. The image of $\tilde{s}$ is the set **KC***, i.e. the set of sequences satisfying the generalized Kummer congruences.*

Remember (Lemma 62) that we had a G-equivariant map
$$s : M(G, \mathbb{Z}_p) \to \mathbf{KC} \subseteq \prod_{k \geq 4}^{*} \mathbb{Q}_p$$
$$\mu \to \left(\int_G x^k d\mu(\bar{x}) \right)^{*}_{k \geq 4}$$
Proposition 111 is an immediate consequence of

Lemma 113. *i) The bijection*
$$\tilde{s} : [KO_p^\wedge, KO_p^\wedge] \xrightarrow{\sim} \mathbf{KC}$$
is G-equivariant.

ii) The diagram
$$\begin{tikzcd} {[KO_p^\wedge, KO_p^\wedge]} \arrow[rr, "\sim", "\eta_5"'] \arrow[dr, "\sim", "\tilde{s}"'] & & M(G, \mathbb{Z}_p) \arrow[dl, "s"] \\ & \mathbf{KC} & \end{tikzcd}$$
is commutative.

Proof. Let $g \in G$, $\alpha \in [KO_p^\wedge, KO_p^\wedge]$ and $k \in \{4, 6, 8, \dots\}$.

i) We have

$$\tilde{s}(g \odot \alpha) = \tilde{s}(KO_p^\wedge \xrightarrow{\alpha} KO_p^\wedge \xrightarrow{\psi^g} KO_p^\wedge) = \Big(\pi_{2k}(\psi^g \circ \alpha)\Big)^*_{k \geq 4}$$

$$= \Big(\pi_{2k}(\psi^g) \cdot \pi_{2k}(\alpha)\Big)^*_{k\geq 4} = \Big(g^k \pi_{2k}(\alpha)\Big)^*_{k \geq 4} = g \odot \big(\pi_{2k}(\alpha)\big)^*_{k\geq 4} = g \odot \tilde{s}(\alpha).$$

ii) Example 9.5 in [AHR] states that

$$\pi_{2k}\alpha = \int_G x^k d\eta_5(\alpha).$$

$\square$

Corollary 114. *The map*

$$s : M(G, \mathbb{Z}_p) \to \mathbf{KC} \subseteq \prod_{k\geq 4}^{*} \mathbb{Q}_p$$

is a bijection.

The characteristic map

To prepare the proof of Part iv) of Theorem 84 in the next paragraph, we now repeat the construction made in Subsection 5.2 of [AHR]. Let $gl_1 S \to X$ be a rational spectrum under $gl_1 S$. The Bousfield localization of X with respect to $M\mathbb{Q}$ is weakly equivalent to $X \otimes \mathbb{Q} \approx X$. Because $\pi_0 gl_1 S = \{\pm 1\}$ we know that

$$* \approx (gl_1 S) \otimes \mathbb{Q} \approx L_{H\mathbb{Q}} gl_1 S.$$

Thus

$$\text{spectra}(gl_1 S, X) \approx \text{spectra}(gl_1 S, L_{H\mathbb{Q}} X) \approx \text{spectra}(L_{H\mathbb{Q}} gl_1 S, L_{H\mathbb{Q}} X) \approx * \,.$$

Inspection of the exact sequences (coming from Definition 97)

$$\mathbf{A}(X) \to \text{spectra}(gl_1 S/string, X) \to \text{spectra}(gl_1 S, X)$$

and

$$\text{spectra}(bstring, X) \to \text{spectra}(gl_1 S/string, X) \to \text{spectra}(gl_1 S, X)$$

gives a weak equivalences

$$\mathbf{A}(X) \approx \text{spectra}(gl_1 S/string, X) \approx \text{spectra}(bstring, X).$$

Because X is rational we have

$$[bstring, X] \cong [bstring, L_{H\mathbb{Q}} X] \cong [L_{H\mathbb{Q}} bstring, L_{H\mathbb{Q}} X] \cong [bstring \otimes \mathbb{Q}, X \otimes \mathbb{Q}].$$

We now use the following facts:

i) The set $\pi_{2k}(bstring \otimes \mathbb{Q})$ is a 1-dimensional $\mathbb{Q}$-vector space for all $k \equiv 0 \mod 2$ with $k \geq 4$.

ii) We have a natural map
$$c : bstring \to bo \to bu$$
where the last map is the complexification map. Let $k \geq 4$ be even. The induced map
$$\pi_{2k}c : \pi_{2k}bstring \to \pi_{2k}bu$$
is an isomorphism of $\mathbb{Z}$-modules. Let $v \in \pi_2 bu$ be the Bott element. Then v^k is a generator of $\pi_{2k}bu$ and we define $v^k_{string} \in \pi_{2k}bstring \subseteq \pi_{2k}(bstring \otimes \mathbb{Q})$ to be the pre-image of v^k, i.e. v^k_{string} is a base for $\pi_{2k}(bstring \otimes \mathbb{Q})$.

We get an isomorphism
$$\hat{s} : [bstring, X] \xrightarrow{\sim} \prod_{k\geq 4}^{*} \pi_{2k}X$$
$$f \mapsto \left((\pi_{2k}f)(v^k_{string})\right)^*_{k\geq 4}.$$

Definition 115 ([AHR], Definition 5.9 and Definition 5.11)**.** If X is a spectrum, let
$$\mathbf{D}(X) := \prod_{k\geq 4}^{*} \pi_{2k}X \otimes \mathbb{Q}.$$
If $gl_1S \to X$ is a spectrum under gl_1S, then the characteristic map
$$b : \pi_0\mathbf{A}(X) \to \mathbf{D}(X)$$
is given by the composition
$$\pi_0\mathbf{A}(X) \to \pi_0\mathbf{A}(X \otimes \mathbb{Q}) \cong [bstring, X \otimes \mathbb{Q}] \xrightarrow{\sim} \prod_{k\geq 4}^{*} \pi_{2k}X \otimes \mathbb{Q} = \mathbf{D}(X)$$
where the first map is the application of the $\pi_0\mathbf{A}(-)$-functor to the canonical map $X \to X \otimes \mathbb{Q}$. With $\mathbf{C}(X) \subseteq \mathbf{D}(X)$ we denote the image of b.

Arithmetic squares

The goal of this paragraph is to prove Part iv) of Theorem 84. Let $c \in \mathbb{Z}_{(p)} \subseteq \mathbb{Z}_p^\times$ be an element which projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$. Let $gl_1S \to X$ be a spectrum under gl_1S. With $X \otimes \mathbb{Q}$ we denote the rationalization of X. Further we define a bijection
$$m_c : \prod_{k\geq 4}^{*} \mathbb{Q}_p \xrightarrow{\sim} \prod_{k\geq 4}^{*} \mathbb{Q}_p$$
by
$$(b_k)^*_{k\geq 4} \mapsto \Big((1-c^k)(1-p^{k-1})b_k\Big)^*_{k\geq 4}.$$
Since $c \in \mathbb{Q}^\times$ we have that $(1-c^k)(1-p^{k-1}) \in \mathbb{Q}^\times$ for all even $k \geq 4$. Therefore m_c fulfil the property that
$$m_c\left(\prod_{k\geq 4}^{*} \mathbb{Q}\right) = \prod_{k\geq 4}^{*} \mathbb{Q}.$$
Again we need

Proposition 116 ([AHR],Proposition 7.10)**.** *Let $c \in \mathbb{Z}_p^\times$ be an element which projects to a generator of $\mathbb{Z}_p^\times/\{\pm 1\}$. The following diagram commutes:*

$$\begin{tikzcd}
\pi_0\mathbf{A}(gl_1(KO_p^\wedge)) \arrow[r, "\eta_{4,c}\circ\eta_3\circ\eta_2"] \arrow[d, "b"', "\cong"] & {[KO_p^\wedge, KO_p^\wedge]} \arrow[r, "\eta_5"] \arrow[d, "\cong"', "\tilde{s}"] & M(G,\mathbb{Z}_p) \arrow[dl, "s"] \\
\mathbf{C}(gl_1(KO_p^\wedge)) \arrow[r] \arrow[d, "\subseteq"] & \mathbf{KC} \arrow[d, "\subseteq"] & \\
\mathbf{D}(gl_1(KO_p^\wedge)) = \prod^*_{k\geq 4}\mathbb{Q}_p \arrow[r, "m_c"'] & \prod^*_{k\geq 4}\mathbb{Q}_p &
\end{tikzcd}$$

where

i) b is the map described in Definition 115.

ii) the upper right triangle is described in Lemma 113.

We now use the fact, that there is a homotopy pull-back square

$$\begin{tikzcd}
KO_{(p)} \arrow[r] \arrow[d] & KO_p^\wedge \arrow[d] \\
KO_{(p)}\otimes\mathbb{Q} \arrow[r] & KO_p^\wedge\otimes\mathbb{Q}
\end{tikzcd}$$

Applying the functor $\pi_0\mathbf{A}(gl_1(-))$ we get a commutative diagram

$$\begin{tikzcd}
\pi_0\mathbf{A}(gl_1(KO_{(p)})) \arrow[r] \arrow[d] & \pi_0\mathbf{A}(gl_1(KO_p^\wedge)) \arrow[d, "b"] \\
\pi_0\mathbf{D}(gl_1(KO_{(p)})) \arrow[r] \arrow[d, "="'] & \pi_0\mathbf{D}(gl_1(KO_p^\wedge)) \arrow[d, "="] \\
\prod^*_{k\geq 4}\mathbb{Q} \arrow[r, "\subseteq"] & \prod^*_{k\geq 4}\mathbb{Q}_p
\end{tikzcd}$$

Together with Proposition 116 we get a commutative diagram

$$\begin{tikzcd}
\pi_0E_\infty(MString, KO_{(p)}) \arrow[r, "\subseteq"] \arrow[d] & \pi_0E_\infty(MString, KO_p^\wedge) \arrow[d, "\eta_1"] \arrow[dr, "\mathrm{ahr}_c"] & \\
\pi_0\mathbf{A}(gl_1(KO_{(p)})) \arrow[r] \arrow[d] & \pi_0\mathbf{A}(gl_1(KO_p^\wedge)) \arrow[r] \arrow[d, "b"] & M(G,\mathbb{Z}_p) \arrow[d, "\cong"', "s"] \\
\prod^*_{k\geq 4}\mathbb{Q} \arrow[r, "\subseteq"] & \prod^*_{k\geq 4}\mathbb{Q}_p \arrow[r, "m_c"'] & \prod^*_{k\geq 4}\mathbb{Q}_p
\end{tikzcd}$$

where s maps a measure μ to the sequence

$$s(\mu) = \left(\int_G \bar{x}^k d\mu\right)^*_{k\geq 4} \in \prod_{k\geq 4}^{*} \mathbb{Z}_p$$

Therefore the image $\mathbf{AHR}_c^{loc}$ of the map

$$\pi_0 E_\infty(MString, KO_{(p)}) \xrightarrow{\subseteq} \pi_0 E_\infty(MString, KO_p^\wedge) \xrightarrow{\mathrm{ahr}_c} M(G, \mathbb{Z}_p)$$

is given by the elements $\mu \in \mathrm{im}(\mathrm{ahr}_c) := \mathbf{AHR}_c$ which fulfil the additional property that

$$s(\mu) = \left(\int_G \bar{x}^k d\mu\right)^*_{k\geq 4} \in m_c\left(\prod_{k\geq 4}^{*} \mathbb{Q}\right) = \prod_{k\geq 4}^{*} \mathbb{Q}.$$

Since

$$\prod_{k\geq 4}^{*} \mathbb{Q} \cap \prod_{k\geq 4}^{*} \mathbb{Z}_p = \prod_{k\geq 4}^{*} \mathbb{Z}_{(p)}$$

this proves Part iv) of Theorem 84.

References

[ABGHR] M. Ando, A. J. Blumberg, D. Gepner, M. J. Hopkins and C. Rezk. Units of ring spectra and thom spectra, available at http://lanl.arxiv.org/abs/0810.4535v2.

[AHR] M. Ando, M. J. Hopkins and C. Rezk. Multiplicative orientations of KO-theory and of the spectrum of topological modular forms. http://www.math.uiuc.edu/∼mando/papers/koandtmf.pdf, 2010. preprint, Version 0.5.

[AHS] J. F. Adams, A. S. Harris, and R. M. Switzer. Hopf algebras of cooperations for real and complex K-theory. Proc. Londan Math. Soc. (3) 23 (1971), 385-408. MR MR0293617 (45 2694)

[B79] A. K. Bousfield. The localization of spectra with respect to homology. Topology 18 (1979), 257-281.

[B87] A. K. Bousfield. Uniqueness of infinite deloopings for K-theoretic spaces. Pacific J. Math., 129(1):1-31,1987

[EKMM] A. D. Elmendorf, I. Kriz, M.A. Mandell, and J.P. May. Rings, modules, and algebras in stable homotopy theory. With an appendix by M. Cole. Mathematical Surveys and Monographs, 47, Providence, R.I: American Mathematical Society. xi, 249 p. [ISBN 0-8218-0638-6/hbk], 1997.

[F] E. M. Friedlander. The infinite loop Adams conjecture via classification theorems for F spaces. Math. Proc. Cambridge Philos. Soc. 87 (1980), no. 1, 109-150. MR MR549303 (81b:55023)

[H] M. J. Hopkins. $K(1)$-local E_∞ ring spectra. unpublished notes, 1998.

[Ka] N. M. Katz. p-adic L-functions via moduli of elliptic curves. Proc. Sympos. Pure Math., 29, Providence, R.I.: American Mathematical Society, pp. 479-506, MR 0432649

[Ko] N. Koblitz. p-adic Numbers, p-adic Analysis, and Zeta-Functions, Second Edition.

[Ku] N. J. Kuhn. Morava K-theories and infinite loop spaces. In Algebraic topology (Arcata, CA, 1986), pages 243-257. Springer, Berlin, 1989.

[Lan] S. Lang. Cyclotomic Fields. Springer, New York - Heidelberg, 1978.

[Laz] M. Lazard. Groupes analytiques p-adiques. Publications mathematiques de l'.I.H.E.S., tome 26 (1965), p. 5-219.

[LMSM] L. G. Lewis, Jr., J. P. May, M. Steinberger, and J. E. McClure. Equivariant stable homotopy therory. Lecture Notes in Mathematics, vol. 1213, Springer-Verlag, Berlin, 1986, With contributions by J. E. McClure. MR0866482 (88e:55002)

[N] J. Neukirch, Algebraic number theory, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 322 , Springer-Verlag, Berlin, 1999.

[R] C. Rezk. The units of a ring spectrum and a logarithmic cohomology operation. J. Amer. Math. Soc., 19(4):969-1014, 2006.

[S] J. P. Serre. Linear Representations of Finite Groups. New York: Springer- Verlag, [ISBN 0-387-90190-6], 1977.

[W] L. C. Washington. Introduction to Cyclotomic Fields. Berlin-Heidelberg-New York: Springer, 1982